Teismo praktikos rinkinys

TEISINGUMO TEISMO (didžioji kolegija) SPRENDIMAS

2020 m. spalio 6 d.*

(Tekstas ištaisytas 2020 m. lapkričio 16 d. nutartimi)

Turinys

* Proceso kalba: prancūzų.

„Prašymas priimti prejudicinį sprendimą – Asmens duomenų tvarkymas elektroninių ryšių sektoriuje – Elektroninių ryšių paslaugų teikėjas – Prieglobos paslaugų ir interneto prieigos paslaugų teikėjai – Bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas – Automatizuota duomenų analizė – Prieiga prie duomenų realiuoju laiku – Nacionalinio saugumo užtikrinimas ir kova su terorizmu – Kova su nusikalstamumu – Direktyva 2002/58/EB – Taikymo sritis – 1 straipsnio 3 dalis ir 3 straipsnis – Elektroninių ryšių konfidencialumas – Apsauga – 5 straipsnis ir 15 straipsnio 1 dalis – Direktyva 2000/31/EB – Taikymo sritis – Europos Sąjungos pagrindinių teisių chartija – 4, 6–8, 11 straipsniai ir 52 straipsnio 1 dalis – ESS 4 straipsnio 2 dalis“

Sujungtose bylose C-511/18, C-512/18 ir C-520/18

dėl *Conseil d'État* (Valstybės Taryba, Prancūzija) 2018 m. liepos 26 d. nutartimis, kurias Teisingumo Teismas gavo 2018 m. rugpjūčio 3 d. (C-511/18 ir C-512/18), ir *Cour constitutionnelle* (Konstitucinis Teismas, Belgija) 2018 m. liepos 19 d. nutartimi, kurią Teisingumo Teismas gavo 2018 m. rugpjūčio 2 d. (C-520/18), pagal SESV 267 straipsnį pateiktų prašymų priimti prejudicinį sprendimą bylose

La Quadrature du Net (C-511/18 ir C-512/18),

French Data Network (C-511/18 ir C-512/18),

Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 ir C-512/18),

Igwan.net (C-511/18)

prieš

Premier ministre (C-511/18 ir C-512/18),

Garde des Sceaux, ministre de la Justice (C-511/18 ir C-512/18),

Ministre de l'Intérieur (C-511/18),

Ministre des Armées (C-511/18), dalyvaujant:

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

ir

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

prieš

Conseil des ministres,

dalyvaujant

Child Focus (C-520/18),

TEISINGUMO TEISMAS (didžioji kolegija),

kurį sudaro pirmininkas K. Lenaerts, pirmininko pavaduotoja R. Silva de Lapuerta, kolegijų pirmininkai J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P. G. Xuereb ir L. S. Rossi, teisėjai J. Malenovský, L. Bay Larsen, T. von Danwitz (pranešėjas), C. Toader, K. Jürimäe, C. Lycourgos ir N. Piçarra,

generalinis advokatas M. Campos Sánchez-Bordona,

posėdžio sekretorė C. Strömholm, administratorė,

atsižvelgęs į rašytinę proceso dalį ir įvykus 2019 m. rugsėjo 9 ir 10 d. posėdžiui,

išnagrinėjęs pastabas, pateiktas:

– *Quadrature du Net*, *Fédération des fournisseurs d'accès à Internet associatifs*, *Igwan.net* ir *Center for Democracy and Technology*, atstovaujamų advokato A. Fitzjean Ò Cobhthaigh,

– *French Data Network*, atstovaujamos advokato Y. Padova,

– *Privacy International*, atstovaujamos advokato H. Roy,

– *Ordre des barreaux francophones ir germanophone*, atstovaujamos advokatų E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart ir J.-F. Henrotte,

– *Académie Fiscale ASBL* ir *UA*, atstovaujamų J.-P. Riquet,

– *Liga voor Mensenrechten ASBL*, atstovaujamos advokato J. Vander Velpen,

– *Ligue des Droits de l'Homme ASBL*, atstovaujamos advokatų R. Jespers ir J. Fermon,

– VZ, WY ir XX, atstovaujamų advokato D. Pattyn,

– *Child Focus*, atstovaujamos advokatų N. Buisseret, K. De Meester ir J. Van Cauter,

– Prancūzijos vyriausybės, iš pradžių atstovaujamos D. Dubois, F. Alabrune, D. Colas, E. de Moustier ir A.-L. Desjonquères, vėliau – D. Dubois, F. Alabrune, E. de Moustier ir A.-L. Desjonquères,

– Belgijos vyriausybės, atstovaujamos J.-C. Halleux, P. Cottin ir C. Pochet, padedamų advokatų J. Vanpraet, Y. Peeters, S. Depré ir E. de Lophem,

– Čekijos vyriausybės, atstovaujamos M. Smolek, J. Vláčil ir O. Serdula,

– Danijos vyriausybės, iš pradžių atstovaujamos J. Nymann-Lindegren, M. Wolff ir P. Ngo, vėliau – J. Nymann-Lindegren ir M. Wolff,

– Vokietijos vyriausybės, iš pradžių atstovaujamos J. Möller, M. Hellmann, E. Lankenau, R. Kanitz ir T. Henze, vėliau – J. Möller, M. Hellmann, E. Lankenau ir R. Kanitz,

– Estijos vyriausybės, atstovaujamos N. Grünberg ir A. Kalbus,

– Airijos vyriausybės, atstovaujamos A. Joyce, M. Browne ir G. Hodge, padedamų BL D. Fennelly,

– Ispanijos vyriausybės, iš pradžių atstovaujamos L. Aguilera Ruiz ir A. Rubio González, vėliau – L. Aguilera Ruiz,

– Kipro vyriausybės, atstovaujamos E. Neofytou,

– Latvijos vyriausybės, atstovaujamos V. Soņeca,

– Vengrijos vyriausybės, iš pradžių atstovaujamos M. Z. Fehér ir Z. Wagner, vėliau – M. Z. Fehér,

– Nyderlandų vyriausybės, atstovaujamos K. Bulterman ir M. A. M. de Ree,

– Lenkijos vyriausybės, atstovaujamos B. Majczyna, J. Sawicka ir M. Pawlicka,

– Švedijos vyriausybės, iš pradžių atstovaujamos H. Shev, H. Eklinder, C. Meyer-Seitz ir A. Falk, vėliau – H. Shev, H. Eklinder, C. Meyer-Seitz ir J. Lundberg,

– Jungtinės Karalystės vyriausybės, atstovaujamos S. Brandon, padedamo QC G. Facenna ir baristerio C. Knight,

– (įtrauka pašalinta 2020 m. lapkričio 16 d. nutartimi)

– Europos Komisijos, iš pradžių atstovaujamos H. Kranenborg, M. Wasmeier ir P. Costa de Oliveira, vėliau – H. Kranenborg ir M. Wasmeier,

– Europos duomenų apsaugos priežiūros pareigūno, atstovaujamo T. Zerdick ir A. Buchta,

susipažinęs su 2020 m. sausio 15 d. posėdyje pateikta generalinio advokato išvada,

priima šį

Sprendimą

1 Prašymai priimti prejudicinį sprendimą pateikti, pirma, dėl 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002, p. 37; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 514), iš dalies pakeistos 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB (OL L 337, 2009, p. 11; klaidų ištaisymai OL L 241, 2013, p. 9 ir OL L 275, 2014, p. 8, toliau – Direktyva 2002/58), 15 straipsnio 1 dalies ir, antra, dėl 2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyvos 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva) (OL 178, 2000, p. 1; 2004 m. specialusis leidimas lietuvių k. 13 sk., 25 t., p. 399) 12–15 straipsnių, siejamų su Europos Sąjungos pagrindinių teisių chartijos (toliau – Chartija) 4, 6–8, 11 straipsniais bei 52 straipsnio 1 dalimi ir ESS 4 straipsnio 2 dalimi, aiškinimo.

2 Prašymas byloje C-511/18 buvo pateiktas nagrinėjant *Quadrature du Net*, *French Data Network*, *Fédération des fournisseurs d'accès à Internet associatifs* ir *Igwan.net* ginčus su *Premier ministre* (Ministras Pirmininkas, Prancūzija), *Garde des Sceaux, ministre de la Justice* (teisingumo ministras, Prancūzija), *ministre de l'Intérieur* (vidaus reikalų ministras, Prancūzija) ir su *ministre des Armées* (ginkluotųjų pajėgų ministras, Prancūzija) dėl *Décret n.º 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement* (2015 m. rugsėjo 28 d. Dekretas Nr. 2015-1185 dėl specialiųjų žvalgybos tarnybų paskyrimo, JORF, 2015 m. rugsėjo 29 d., dokumentas Nr. 1 iš 97, toliau – Dekretas Nr. 2015-1185), dėl *Décret n.º 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (2015 m. spalio 1 d. Dekretas Nr. 2015-1211 dėl ginčų, susijusių su žvalgybos būdų, kuriems reikalingas leidimas, ir valstybės saugumui svarbių rinkmenų sistemų įgyvendinimu, JORF, 2015 m. spalio 2 d., dokumentas Nr. 7 iš 108, toliau – Dekretas Nr. 2015-1211), dėl *Décret*

n.º 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure pris en application de l'article L. 811-4 du code de la sécurité intérieure (2015 m. gruodžio 11 d. Dekretas Nr. 2015-1639 dėl kitų nei specializuotų žvalgybos tarnybų, kurios gali naudotis Vidaus saugumo kodekso VIII knygos V antraštinėje dalyje nurodytais duomenų rinkimo būdais, paskyrimo, priimto taikant Vidaus saugumo kodekso L. 811-4 straipsnį, JORF, 2015 m. gruodžio 12 d., dokumentas Nr. 28 iš 127, toliau – Dekretas Nr. 2015-1639), taip pat dėl *Décret n.º 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement* (2016 m. sausio 29 d. Dekretas Nr. 2016-67 dėl informacijos rinkimo būdų, JORF, 2016 m. sausio 31 d., dokumentas Nr. 2 iš 113, toliau – Dekretas Nr. 2016-67) teisėtumo.

3 Prašymas byloje C-512/18 buvo pateiktas nagrinėjant *French Data Network*, *Quadrature du Net* ir *Fédération des fournisseurs d'accès à Internet associatifs* ginčus su *Premier ministre* (Ministras Pirmininkas, Prancūzija) ir *Garde des Sceaux, ministre de la Justice* (teisingumo ministras, Prancūzija) dėl *Code des postes et des communications électroniques* (Pašto ir elektroninių ryšių kodeksas, toliau – CPCE) R. 10-13 straipsnio ir dėl *Décret nº 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (2011 m. vasario 25 d. Dekretas Nr. 2011-219 dėl duomenų, leidžiančių nustatyti visų kuriant internete skelbiamą turinį prisidėjusių asmenų tapatybę, saugojimo ir perdavimo, JORF, 2011 m. kovo 1 d., dokumentas Nr. 32 iš 170, toliau – Dekretas Nr. 2011-219) teisėtumo.

4 Prašymas byloje C-520/18 buvo pateiktas nagrinėjant *Ordre des barreaux francophones et germanophone*, *Académie Fiscale ASBL*, *UA*, *Liga voor Mensenrechten ASBL*, *Ligue des Droits de l'Homme ASBL*, VZ, WY ir XX ginčus su *Conseil des ministres* (Ministrų taryba, Belgija) dėl *Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques* (2016 m. gegužės 29 d. Įstatymas dėl duomenų rinkimo ir saugojimo elektroninių ryšių sektoriuje, *Moniteur belge*, 2016 m. liepos 18 d., p. 44717, toliau – 2016 m. gegužės 29 d. įstatymas) teisėtumo.

Teisinis pagrindas

Sąjungos teisė

Direktyva 95/46

5 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 281, 1995, p. 31; 2004 m. specialusis leidimas lietuvių k. 13 sk., 15 t., p. 355) nuo 2018 m. gegužės 25 d. buvo panaikinta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (OL L 119, 2016, p. 1; klaidų ištaisymas OL L 127, 2018, p. 2). Direktyvos 95/46 3 straipsnio 2 dalyje buvo nustatyta:

„Ši direktyva netaikoma tvarkant asmens duomenis:

– kai yra užsiimama tokia veikla, kuri nepatenka į Bendrijos teisės taikymo sritį, kaip antai veikla, kuri numatyta Europos Sąjungos sutarties V ir VI dalyse, taip pat kai atliekamos tvarkymo operacijos, susijusios su visuomenės saugumu, gynyba, valstybės saugumu (taip pat ir valstybės ekonomine gerove, kai tvarkymo operacija susijusi su valstybės saugumo klausimais) ir su valstybės veiksmais baudžiamosios teisės srityje;

– kai duomenis tvarko fizinis asmuo, užsiimdamas tik asmenine ar namų ūkio veikla.“

6 Direktyvos 95/46 III skyriaus „Teisės gynimo būdai, turtinė atsakomybė [atsakomybė] ir sankcijos“ 22 straipsnis buvo suformuluotas taip:

„Nepažeidžiant jokių nuostatų dėl administracinio poveikio priemonių, kurios, *inter alia*, gali būti numatytos prieš perduodant klausimą 28 straipsnyje nurodytai priežiūros institucijai ir [Nedarant poveikio galimybei imtis bet kokių administracinių teisių gynimo priemonių, be kita ko, 28 straipsnyje nurodytoje priežiūros institucijoje,] prieš kreipiantis į teismo instituciją, valstybės narės numato, kad kiekvienas asmuo turi teisę į teisminę gynybą, jei pažeidžiamos teisės, kurias jam garantuoja nacionaliniai įstatymai, taikomi tvarkant tam tikru aptariamu būdu.“

Direktyva 97/66

7 1997 m. gruodžio 15 d. Europos Parlamento ir Tarybos direktyvos 97/66/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (OL L 24, 1997, p. 1) 5 straipsnyje „Pranešimų konfidencialumas“ nustatyta:

„1. Valstybės narės teisės aktais užtikrina pranešimų, perduodamų per viešųjų telekomunikacijų tinklą ar teikiant viešas telekomunikacijų paslaugas, konfidencialumą. Visų pirma jos draudžia asmenims, kurie nėra naudotojai, be atitinkamų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus, išskyrus atvejus, kai tai galima teisėtai daryti pagal 14 straipsnio 1 dalį.

2. Šio straipsnio 1 dalis neturi jokio poveikio teisėtam pranešimų įrašymui, kuris atliekamas teisėtos verslo praktikos metu, kad būtų galima pateikti komercinio sandorio ar kitokių verslo pranešimų įrodymus.“

Direktyva 2000/31

8 Direktyvos 2000/31 14 ir 15 konstatuojamosiose dalyse nustatyta:

„(14) Asmenų [fizinių asmenų] apsaugą tvarkant asmens duomenis reglamentuoja tik [Direktyva 95/46] ir [Direktyva 97/66], kurios visapusiškai taikomos informacinės visuomenės paslaugoms; šios direktyvos jau sukuria Bendrijos teisinę bazę asmens duomenų srityje, todėl nebūtina reglamentuoti šio klausimo šioje direktyvoje, kad būtų užtikrintas sklandus vidaus rinkos funkcionavimas, ypač laisvas asmens duomenų judėjimas tarp valstybių narių; ši direktyva turėtų būti įgyvendinama ir taikoma vadovaujantis visais principais, susijusiais su asmens duomenų apsauga, ypač dėl neužsakytų komercinių pranešimų ir tarpininkų atsakomybės; ši direktyva negali užkirsti kelio anonimiškai naudotis atviraisiais tinklais, pavyzdžiui, internetu.

(15) Pranešimų slaptumą garantuoja Direktyvos [97/66] 5 straipsnis; pagal tą direktyvą valstybės narės privalo drausti asmenims, kurie nėra siuntėjai ir gavėjai, kaip nors perimti arba sekti tokius pranešimus, nebent jie turėtų teisėtus leidimus.“

9 Direktyvos 2000/31 1 straipsnis suformuluotas taip:

„1. Šia direktyva siekiama prisidėti prie tinkamo vidaus rinkos funkcionavimo užtikrinant laisvą informacinės visuomenės paslaugų judėjimą tarp valstybių narių.

2. Šia direktyva derinamos, kiek reikalinga 1 dalyje nustatytiems tikslams pasiekti, kai kurios nacionalinės nuostatos dėl informacinės visuomenės paslaugų, susijusios su vidaus rinka, paslaugų teikėjų steigimusi, komerciniais pranešimais, elektroninėmis sutartimis, tarpininkų atsakomybe, elgesio kodeksais, ginčų nagrinėjimo ne teismo tvarka, teisminėmis priemonėmis ir valstybių narių bendradarbiavimu.

3. Ši direktyva papildo Bendrijos teisę, taikytiną informacinės visuomenės paslaugoms, nepažeisdama apsaugos, ypač visuomenės sveikatos ir vartotojų interesų, lygio, numatyto Bendrijos teisės aktuose ir juos įgyvendinančiuose nacionaliniuose įstatymuose, ir [jeigu tai] neriboja laisvės teikti informacinės visuomenės paslaugas.

<…>

5. Ši direktyva netaikoma:

<…>

b) sprendžiant klausimus, susijusius su informacinės visuomenės paslaugomis, kurias reglamentuoja [direktyvos 95/46 ir 97/66];

<…>“

10 Direktyvos 2000/31 2 straipsnis suformuluotas taip:

„Šioje direktyvoje šios sąvokos turi tokią reikšmę:

a) „informacinės visuomenės paslaugos“ – tai paslaugos, apibūdintos [1998 m. birželio 22 d. Europos Parlamento ir Tarybos direktyvos 98/34/EB, nustatančios informacijos apie techninius standartus ir reglamentus teikimo tvarką (OL L 204, 1998, p. 37, 2004 m. specialusis leidimas lietuvių k. 13 sk., 20 t., p. 337)], su pakeitimais, padarytais [1998 m. liepos 20 d. Europos Parlamento ir Tarybos direktyva 98/48/EB (OL L 217, 1998, p. 18, 2004 m. specialusis leidimas lietuvių k. 13 sk., 21 t., p. 8)], 1 straipsnio 2 dalyje;

<…>“

11 Direktyvos 2000/31 15 straipsnyje numatyta:

„1. Valstybės narės nenustato teikėjams nei bendros prievolės teikiant 12, 13 ir 14 straipsnių reglamentuojamas paslaugas stebėti informaciją, kurią jie perduoda arba saugo, nei bendros prievolės aktyviai domėtis faktais arba aplinkybėmis, rodančiomis nelegalią veiklą.

2. Valstybės narės gali nustatyti prievoles informacinės visuomenės paslaugų teikėjams nedelsiant informuoti kompetentingas viešąsias institucijas apie įtariamą nelegalią veiklą arba informaciją, kurią pateikia jų paslaugų gavėjai, arba prievolę pateikti kompetentingoms institucijoms, gavus jų prašymą, informaciją, leidžiančią nustatyti jų paslaugos gavėjų, su kuriais jie sudarę informacijos saugojimo sutartis, tapatybę.“

Direktyva 2002/21

12 2002 m. kovo 7 d. Europos Parlamento ir Tarybos direktyvos 2002/21/EB dėl elektroninių ryšių tinklų ir paslaugų bendrosios reguliavimo sistemos (Pagrindų direktyva) (OL L 108, 2002, p. 33; 2004 m. specialusis leidimas lietuvių k., 13 sk., 29 t., p. 349) 10 konstatuojamoje dalyje nustatyta:

„Apibrėžimas „Informacinės visuomenės paslaugos“, pateiktas [Direktyvos 98/34], pakeistos [Direktyva 98/48], 1 straipsnyje, apima plačią ekonominę veiklą, kuri vyksta operatyviniu kompiuteriniu ryšiu. Didžiajai tokios veiklos daliai ši direktyva netaikoma, nes tokios veiklos, visos ar tam tikros jos dalies, nesudaro signalų perdavimas elektroninių ryšių tinklais. Balso telefonijai ir elektroninio pašto

perdavimo paslaugoms ši direktyva taikoma. Ta pati įmonė, pavyzdžiui, interneto paslaugų teikėja, gali teikti ir elektroninių ryšių paslaugą, tokią kaip prieiga prie interneto, ir paslaugas, kurioms ši direktyva netaikoma, tokias kaip turinio teikimas internetu.“

13 Direktyvos 2002/21 2 straipsnyje numatyta:

„Šioje direktyvoje:

<…>

c) „elektroninių ryšių paslauga“ – paslauga, paprastai teikiama už atlygį, kuri visa ar didžiąja dalimi susideda iš signalų perdavimo elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo paslaugas tinklais, naudojamais transliavimui, išskyrus elektroniniais ryšių tinklais ir paslaugomis perduodamo turinio teikimo ar redakcinės jo kontrolės paslaugas; į šią paslaugą neįeina informacinės visuomenės paslaugos, apibrėžtos Direktyvos [98/34] 1 straipsnyje, kurios visos ar didžiąja dalimi susideda iš signalų perdavimo elektroninių ryšių tinklais;

<…>“

Direktyva 2002/58

14 Direktyvos 2002/58 2, 6, 7, 11, 22, 26 ir 30 konstatuojamosiose dalyse nustatyta:

„(2) Šia direktyva siekiama gerbti pagrindines žmogaus teises ir laikomasi [Chartijos] principų; visų pirma šia direktyva siekiama užtikrinti visapusišką pagarbą minėtos Chartijos 7 ir 8 straipsniuose išdėstytoms teisėms.

<…>

(6) Internetas keičia tradicines rinkos struktūras sukurdamas bendrą, pasaulinę infrastruktūrą įvairioms elektroninių ryšių paslaugoms teikti. Viešai prieinamos elektroninių ryšių interneto paslaugos atveria naujas galimybes naudotojams, bet dėl jų taip pat iškyla [nauja] rizika asmens duomenims ir privatumui.

(7) Viešiesiems ryšių tinklams reikėtų nustatyti specifines teisines, normines ir technines nuostatas, kad būtų apsaugotos fizinių asmenų pagrindinės teisės ir laisvės bei juridinių asmenų teisėti interesai, visų p[ir]ma dėl didėjančių automatinio duomenų, susijusių su abonentais ir naudotojais, kaupimo ir tvarkymo pajėgumų.

<…>

(11) Ši direktyva, kaip ir Direktyva [95/46], nenagrinėja pagrindinių teisių ir laisvių apsaugos klausimų, susijusių su veiklos rūšimis, kurių nereglamentuoja [Sąjungos] teisės aktai. Todėl ji nekeičia esamos pusiausvyros tarp fizinio asmens teisės į privatumą ir valstybių narių galimybės imtis šios direktyvos 15 straipsnio 1 dalyje nurodytų priemonių, kurių reikia užtikrinti visuomenės saugumą, gynybą, valstybės saugumą (įskaitant valstybės ekonominę gerovę, kai veiklos rūšys yra susijusios su valstybės saugumo klausimais) ir baudžiamosios teisės vykdymu. Tokiu būdu ši direktyva neturi jokio poveikio valstybių narių galimybėms teisėtu būdu perimti elektroninių ryšių pranešimus arba imtis kitų priemonių, kurių reikia minėtiems tikslams pasiekti laikantis Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos [pasirašytos 1950 m. lapkričio 4 d. Romoje], kaip išaiškinta Europos žmogaus teisių teismo nutarime [kaip ją savo sprendimuose aiškina Europos Žmogaus Teisių Teismas]. Tokios priemonės turi būti tinkamos, griežtai

atitinkančios siekiamą tikslą ir būtinos demokratinėje visuomenėje, taip pat joms turi būti taikoma tinkama apsaugos garantija pagal Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją.

<…>

(22) Draudimas saugoti pranešimus ir srauto duomenis kitiems nei naudotojai asmenims, taip pat saugoti juos be naudotojų sutikimo nėra skirtas uždrausti šios informacijos automatinį, tarpinį ir tranzitinį saugojimą, jeigu tai daroma tik siekiant perduoti pranešimą elektroninių ryšių tinklu, ir ne ilgiau, nei reikia perdavimui ir srautams valdyti, garantuojant konfidencialumą saugojimo metu. <…>

<…>

(26) Su abonentais susiję duomenys, kurie yra tvarkomi elektroninių ryšių tinkluose sujungimų ir informacijos perdavimo tikslais, apima duomenis apie fizinių asmenų privatų gyvenimą ir susiję su jų teise į susirašinėjimo slaptumą arba susiję su teisėtais juridinių asmenų interesais. Tokie duomenys saugotini tiek, kiek jie reikalingi [paslaugai teikti,] sąskaitoms pateikti ir sumokėti už tinklų sujungimus, ir tik ribotą laiko tarpą. <…> [Bet koks kitas tokių duomenų tvarkymas] leidžiama[s] tik abonentui sutikus, kuris apsisprendžia, remdamasis tikslia ir išsamia informacija iš šio teikėjo apie numatomus duomenų tolimesnio tvarkymo būdus, apie abonento teisę nesutikti arba panaikinti duotą sutikimą tvarkyti tokius duomenis. <…> sunaikinami arba padaromi anoniminiais tokioms paslaugoms [ryšių paslaugoms rinkodaros tikslais] reikalingi srauto duomenys. <…>

<…>

(30) Elektroninių ryšių tinklų ir paslaugų teikimo sistemos turi būti suprojektuotos taip, kad reikalingas asmens duomenų kiekis būtų griežtai apribotas iki minimumo. <…>“

15 Direktyvos 2002/58 1 straipsnyje „Taikymo sritis ir tikslas“ nustatyta:

„1. Šioje direktyvoje numatytas valstybių narių nuostatų, užtikrinančių vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatumą ir konfidencialumą, apsaugą, susijusių [kiek tai susiję] su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, ir užtikrinančių laisvą tokių duomenų judėjimą ir laisvą elektroninių ryšių įrangos ir paslaugų judėjimą [Europos Sąjungoje], suderinimas.

2. Šios direktyvos nuostatos smulkiau išaiškina [patikslina] ir papildo Direktyvą [95/46] šio straipsnio pirmoje dalyje nurodytais tikslais. Be to, jos numato abonentų, kurie yra juridiniai asmenys, teisėtų interesų apsaugą.

3. Ši direktyva netaikoma veiklos rūšims, kurios neįeina į [SESV] taikymo sritį, tokioms, kurios nurodytos Europos Sąjungos steigimo [Europos Sąjungos] sutarties V ir VI antraštinėse dalyse, ir visais atvejais veiklos rūšims, susijusioms su visuomenės saugumu, gynyba, valstybės saugumu (įskaitant valstybės ekonominę gerovę, kai atitinkamos veiklos rūšys yra susijusios su valstybės saugumo klausimais) bei valstybės veiksmais baudžiamosios teisės srityje.“

16 Direktyvos 2002/58 2 straipsnyje „Sąvokų apibrėžimai“ nurodyta:

„Jeigu toliau nepateikta kitaip, šioje direktyvoje vartojamos sąvokos yra apibrėžiamos taip, kaip apibrėžta Direktyvoje [95/46] ir Direktyvoje [2002/21].

Šioje direktyvoje:

a) „naudotojas“ – tai bet kuris fizinis asmuo, vartojantis viešai prieinamą elektroninių ryšių paslaugą privačiais ar verslo tikslais, ir nebūtinai tai darantis išankstinio paslaugos užsakymo būdu;

b) „srauto duomenys“ – tai duomenys, tvarkomi pranešimui perduoti elektroninių ryšių tinklu, taip pat sąskaitoms už tokį perdavimą pateikti;

c) „vietos nustatymo duomenys“ – elektroninių ryšių tinkluose arba elektroninių ryšių paslaugų teikimo metu tvarkomi duomenys, nurodantys viešosios elektroninių ryšių paslaugos gavėjo galinių įrenginių geografinę padėtį;

d) „pranešimas“ – tai informacija, kuria apsikeičiama arba kuri perduodama tarp baigtinio skaičiaus šalių, naudojantis viešai prieinamomis elektroninių ryšių paslaugomis. Jam nepriskiriama informacija, perduodama kaip dalis viešojo transliavimo paslaugos, naudojant elektroninių ryšių tinklus, išskyrus tuos atvejus, kai tokia informacija gali būti susijusi su informaciją gaunančiu abonentu arba naudotoju, kurio tapatybę galima nustatyti;

<…>“

17 Direktyvos 2002/58 3 straipsnyje „Paslaugos“ numatyta:

„Ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su viešųjų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais Bendrijoje, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius.“

18 Direktyvos 2002/58 5 straipsnyje „Pranešimų konfidencialumas“ nustatyta:

„1. Valstybės narės užtikrina pranešimų ir su jais susijusių srauto duomenų, perduodamų per viešųjų ryšių tinklą ir teikiant viešai teikiamas elektroninių ryšių paslaugas, konfidencialumą, taikydamos nacionalinės teisės aktus. Visų pirma jos draudžia [asmenims, kurie nėra naudotojai] be atitinkamų naudotojų sutikimo klausytis, įrašyti, kaupti ar kitu būdu perimti bei stebėti pranešimus ir su jais susijusius srauto duomenis, išskyrus atvejus, kai tai galima teisėtai daryti pagal 15 straipsnio 1 dalį. Šios dalies nuostatos nedraudžia techninio saugojimo, būtino perduoti pranešimą nepažeidžiant konfidencialumo principo.

<…>

3. Valstybės narės užtikrina, kad saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija abonento ar naudotojo galiniame įrenginyje būtų leidžiama tik su sąlyga, jei atitinkamam abonentui ar naudotojui sutikus pagal Direktyvą [95/46] pateikiama aiški ir išsami informacija, *inter alia*, apie tokio duomenų tvarkymo tikslus [abonentas ar naudotojas, gavęs pagal Direktyvą [95/46] išsamią informaciją, *inter alia*, apie tokio duomenų tvarkymo tikslus, su tuo sutiko]. Ši nuostata nedraudžia vykdyti techninį saugojimą ar naudotis duomenimis, jei siekiama tik atlikti pranešimo perdavimą elektroninių ryšių tinklu, taip pat [arba] būtinais atvejais, kad informacinės visuomenės paslaugų teikėjas galėtų teikti paslaugas, kurių aiškiai paprašo abonentas ar naudotojas.“

19 Direktyvos 2002/58 6 straipsnyje „Srauto duomenys“ numatyta:

„1. Su abonentais ir naudotojais susiję srauto duomenys, kuriuos tvarko ir saugo viešųjų ryšių tinklo ar viešai prieinamų elektroninių ryšių paslaugų teikėjas, turi būti sunaikinti arba pakeisti taip, kad taptų anoniminiais, kai šie duomenys nebėra reikalingi pranešimui perduoti, jeigu nepažeidžiamos šio straipsnio 2, 3 ir 5 dalių ir 15 straipsnio 1 dalies nuostatos.

2. Srauto duomenys gali būti tvarkomi, kai reikia abonentams pateikti sąskaitas ir atsiskaityti už tinklų sujungimą. Toks tvarkymas leistinas tol, kol nepasibaigęs terminas, per kurį sąskaita gali būti teisėtai užginčyta ar išieškotas apmokėjimas.

3. Elektroninių ryšių paslaugų rinkodaros arba pridėtinės vertės paslaugų teikimo tikslais viešųjų elektroninių ryšių paslaugų teikėjas gali tvarkyti 1 dalyje nurodytus duomenis tokia apimtimi ir tiek laiko, kiek būtina tokių paslaugų teikimui ar rinkodarai, jeigu abonentas ar naudotojas, su kuriuo duomenys yra susiję, yra iš anksto davęs sutikimą. Naudotojams ar abonentams sudaroma galimybė bet kuriuo metu atšaukti duotą sutikimą srauto duomenims tvarkyti.

<…>

5. Tvarkyti srauto duomenis pagal šio straipsnio 1, 2, 3 ir 4 dalis leidžiama tik asmenims, kurie veikdami pagal viešųjų ryšių tinklų ar viešai prieinamų elektroninių ryšių paslaugų teikėjų įgaliojimą pateikia sąskaitas, valdo srautą, teikia informaciją klientams, nustato sukčiavimo atvejus, vykdo elektroninių ryšių paslaugų rinkodarą arba teikia pridėtinės vertės paslaugas. Šie asmenys gali atlikti tik tokius veiksmus, kurie yra būtini minėtos veiklos tikslams pasiekti.“

20 Šios direktyvos 9 straipsnio „Vietos nustatymo duomenys, nesudarantys srauto duomenų“ 1 dalyje numatyta:

„Kai vietos nustatymo duomenys, nesudarantys srauto duomenų, susiję su viešųjų ryšių tinklų ar viešųjų elektroninių ryšių naudotojais ar abonentais, gali būti tvarkomi, juos galima tvarkyti tik jeigu jie yra pakeisti taip, kad taptų anoniminiais, arba jeigu naudotojai ar abonentai sutinka su tokiu tvarkymu tokia apimtimi ir tiek laiko, kiek yra būtina teikti pridėtinės vertės paslaugai. Prieš gaudamas sutikimą, paslaugų teikėjas turi informuoti naudotojus ar abonentus apie tai, kokie vietos nustatymo duomenys, nesudarantys srauto duomenų, bus tvarkomi, kokiais tikslais ir kiek laiko, taip pat ar šie duomenys bus perduoti trečiajai šaliai pridėtinės vertės paslaugai teikti. <…>“

21 Minėtos direktyvos 15 straipsnyje „Kai kurių Direktyvos [95/46] nuostatų taikymas“ nustatyta:

„1. Valstybės narės gali patvirtinti teisines [teisėkūros] priemones, ribojančias šios direktyvos 5 ir 6 straipsniuose, 8 straipsnio 1, 2, 3 ir 4 dalyse ir 9 straipsnyje nustatytų teisių ir pareigų taikymą, jeigu toks ribojimas yra būtina, tinkama ir adekvati [proporcinga] demokratinės visuomenės [demokratinėje visuomenėje] priemonė, skirta apsaugoti nacionalinį saugumą (t. y. valstybės saugumą), gynybą, visuomenės saugumą, taip užkardant, tiriant ir nustatant baudžiamąsias veikas ar neteisėtą elektroninių ryšių sistemos naudojimą [taip pat užtikrinti baudžiamųjų veikų prevenciją, tyrimą, atskleidimą ir baudžiamąjį persekiojimą už jas], kaip nurodyta Direktyvos [95/46] 13 straipsnio 1 dalyje. Valstybės narės gali, *inter alia*, patvirtinti teisines [teisėkūros] priemones, leidžiančias ribotą laikotarpį saugoti duomenis, remiantis šioje dalyje nustatytais motyvais. Visos šioje dalyje nurodytos priemonės turi atitikti bendruosius [Sąjungos] teisės principus, tarp jų ir nurodytus Europos Sąjungos Sutarties 6 straipsnio 1 ir 2 dalyse.

<…>

2. Direktyvos [95/46] III skyriaus nuostatos dėl teisės gynimo būdų, atsakomybės ir sankcijų taikomos atsižvelgiant į pagal šią direktyvą priimtas nacionalines nuostatas bei atsižvelgiant į pagal šią direktyvą įgytas atskiras teises.

<…>“

Reglamentas 2016/679

22 Reglamento 2016/679 10 konstatuojamojoje dalyje nustatyta:

„[S]iekiant užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą ir pašalinti asmens duomenų judėjimo Sąjungoje kliūtis, visose valstybėse narėse turėtų būti užtikrinama lygiavertė asmenų teisių ir laisvių apsauga tvarkant tokius duomenis. Visoje Sąjungoje turėtų būti užtikrintas nuoseklus ir vienodas taisyklių, kuriomis reglamentuojama fizinių asmenų pagrindinių teisių ir laisvių apsauga tvarkant asmens duomenis, taikymas. <…>“

23 Šio reglamento 2 straipsnyje nustatyta:

„1. Šis reglamentas taikomas asmens duomenų tvarkymui, visiškai arba iš dalies atliekamam automatizuotomis priemonėmis, ir asmens duomenų, kurie sudaro susisteminto rinkinio dalį ar yra skirti ją sudaryti, tvarkymui ne automatizuotomis priemonėmis.

2. Šis reglamentas netaikomas asmens duomenų tvarkymui, kai:

a) duomenys tvarkomi vykdant veiklą, kuriai Sąjungos teisė netaikoma;

b) duomenis tvarko valstybės narės, vykdydamos veiklą, kuriai taikomas ES sutarties V antraštinės dalies 2 skyrius;

<…>

d) duomenis tvarko kompetentingos valdžios institucijos nusikalstamų veikų prevencijos, tyrimo, nustatymo ar patraukimo baudžiamojon atsakomybėn už jas, baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais.

<…>

4. Šis reglamentas nedaro poveikio Direktyvos [2000/31], visų pirma tos direktyvos 12–15 straipsniuose nustatytų taisyklių dėl tarpininkavimo paslaugų teikėjų atsakomybės, taikymui.

24 Minėto reglamento 4 straipsnyje numatyta:

„Šiame reglamente:

1) asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius;

2) duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas;

<…>“

25 Reglamento 2016/679 5 straipsnyje nustatyta:

„1. Asmens duomenys turi būti:

a) duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);

b) renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu; tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal 89 straipsnio 1 dalį nėra laikomas nesuderinamu su pirminiais tikslais (tikslo apribojimo principas);

c) adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (duomenų kiekio mažinimo principas);

d) tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo paskirtį, būtų nedelsiant ištrinami arba ištaisomi (tikslumo principas);

e) laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi; asmens duomenis galima saugoti ilgesnius laikotarpius, jeigu asmens duomenys bus tvarkomi tik archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal 89 straipsnio 1 dalį, įgyvendinus atitinkamas technines ir organizacines priemones, kurių reikalaujama šiuo reglamentu siekiant apsaugoti duomenų subjekto teises ir laisves (saugojimo trukmės apribojimo principas);

f) tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas).

<…>“

26 Šio reglamento 6 straipsnis suformuluotas taip:

„1. Duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų, ir tik tokiu mastu, kokiu ji yra taikoma:

<…>

c) tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė;

<…>

3. 1 dalies c ir e punktuose nurodytas duomenų tvarkymo pagrindas nustatomas:

a) Sąjungos teisėje; arba

b) duomenų valdytojui taikomoje valstybės narės teisėje.

Duomenų tvarkymo tikslas nustatomas tame teisiniame pagrinde <…>. Tame teisiniame pagrinde galėtų būti išdėstytos konkrečios nuostatos pagal šį reglamentą taikomų taisyklių pritaikymui, įskaitant bendrąsias sąlygas, reglamentuojančias duomenų valdytojo atliekamo duomenų tvarkymo teisėtumą, tvarkytinų duomenų rūšis, atitinkamus duomenų subjektus, subjektus, kuriems asmens duomenys gali

būti atskleisti[,] ir tikslus, dėl kurių asmens duomenys gali būti atskleisti, tikslo apribojimo principą, saugojimo laikotarpius ir duomenų tvarkymo operacijas bei duomenų tvarkymo procedūras, įskaitant priemones, kuriomis būtų užtikrintas teisėtas ir sąžiningas duomenų tvarkymas, kaip antai tas, kurios skirtos kitiems specialiems IX skyriuje numatytiems duomenų tvarkymo atvejams. Sąjungos arba valstybės narės teisė atitinka viešojo intereso tikslą ir yra proporcinga teisėtam tikslui, kurio siekiama.

<…>“

27 Minėto reglamento 23 straipsnyje numatyta:

„1. Sąjungos ar valstybės narės teis[ės], kuri taikoma duomenų valdytojui arba duomenų tvarkytojui, teisėkūros priemone gali būti apribotos 12–22 straipsniuose ir 34 straipsnyje, taip pat 5 straipsnyje tiek, kiek jo nuostatos atitinka 12–22 straipsniuose numatytas teises ir prievoles, nustatytos prievolės ir teisės, kai tokiu apribojimu gerbiama [paisoma] pagrindinių teisių ir laisvių esmė ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti:

a) nacionalinį saugumą;

b) gynybą;

c) visuomenės saugumą;

d) nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar patraukimą už jas baudžiamojon atsakomybėn arba bausmių vykdymą, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją;

e) kitus Sąjungos ar valstybės narės svarbius tikslus, susijusius su bendrais viešaisiais interesais, visų pirma svarbiu ekonominiu ar finansiniu Sąjungos ar valstybės narės interesu, įskaitant pinigų, biudžeto bei mokesčių klausimus, visuomenės sveikatą ir socialinę apsaugą;

f) teismų nepriklausomumo ir teismo procesų apsaugą;

g) reglamentuojamųjų profesijų etikos pažeidimų prevenciją, tyrimą, nustatymą ir patraukimą baudžiamojon atsakomybėn [atsakomybėn] už juos;

h) stebėsenos, tikrinimo ar reguliavimo funkciją, kuri (net jeigu tik kartais) yra susijusi su viešosios valdžios funkcijų vykdymu a–e ir g punktuose nurodytais atvejais;

i) duomenų subjekto apsaugą arba kitų asmenų teisių ir laisvių apsaugą;

j) civilinių ieškinių vykdymo užtikrinimą.

2. Visų pirma visose 1 dalyje nurodytose teisėkūros priemonėse pateikiamos konkrečios nuostatos, susijusios tam tikrais atvejais bent su:

a) duomenų tvarkymo tikslais arba duomenų tvarkymo kategorijomis;

b) asmens duomenų kategorijomis;

c) nustatytų apribojimų apimtimi;

d) apsaugos priemonėmis, kuriomis siekiama užkirsti kelią piktnaudžiavimui arba neteisėtam susipažinimui su duomenimis ar jų perdavimui;

e) duomenų valdytojo arba duomenų valdytojų kategorijų apibūdinimu;

f) saugojimo laikotarpiais ir taikytinomis apsaugos priemonėmis, atsižvelgiant į duomenų tvarkymo arba duomenų tvarkymo kategorijų pobūdį, aprėptį ir tikslus;

g) pavojais duomenų subjektų teisėms ir laisvėms ir

h) duomenų subjektų teise būti informuotiems apie apribojimą, nebent tai pakenktų apribojimo tikslui.“

28 Minėto Reglamento 79 straipsnio 1 dalyje nustatyta:

„Nedarant poveikio galimybei imtis bet kokių galimų administracinių arba neteisminių teisių gynimo priemonių, įskaitant teisę pateikti skundą priežiūros institucijai pagal 77 straipsnį, kiekvienas duomenų subjektas turi teisę imtis veiksmingų teisminių teisių gynimo priemonių, jeigu mano, kad šiuo reglamentu nustatytos jo teisės buvo pažeistos, nes jo asmens duomenys buvo tvarkomi pažeidžiant šį reglamentą.“

29 Reglamento 2016/679 94 straipsnyje numatyta:

„1. Direktyva [95/46] panaikinama nuo 2018 m. gegužės 25 d.

2. Nuorodos į panaikintą direktyvą laikomos nuorodomis į šį reglamentą. Nuorodos į Direktyvos [95/46] 29 straipsniu įsteigtą Darbo grupę asmenų apsaugai tvarkant asmens duomenis laikomos nuorodomis į šiuo reglamentu įsteigtą Europos duomenų apsaugos valdybą.“

30 Šio reglamento 95 straipsnyje nustatyta:

„Šiuo reglamentu fiziniams arba juridiniams asmenims nenustatoma papildomų prievolių, susijusių su duomenų tvarkymu Sąjungoje viešaisiais ryšių tinklais teikiant viešai prieinamas elektroninių ryšių paslaugas, kiek tai susiję su klausimais, kuriais jiems taikomos Direktyvoje [2002/58] nustatytos specialios prievolės, kuriomis siekiama to paties tikslo.“

Prancūzijos teisė

Vidaus saugumo kodeksas

31 *Code de la sécurité intérieure* (Vidaus saugumo kodeksas, toliau – CSI) įstatyminės dalies VIII knygos L. 801-1–L. 898-1 straipsniuose numatytos su žvalgyba susijusios taisyklės.

32 CSI L. 811-3 straipsnyje nurodyta:

„Vien savo atitinkamoms užduotims įgyvendinti specializuotos žvalgybos tarnybos gali naudotis šios knygos V antraštinėje dalyje nurodytais būdais, siekdamos rinkti informaciją apie gynybą ir propaguoti šiuos pagrindinius tautos interesus:

1° nacionalinį nepriklausomumą, teritorijos vientisumą ir nacionalinę gynybą;

2° svarbiausius užsienio politikos interesus, Prancūzijos europinių ir tarptautinių įsipareigojimų vykdymą ir bet kokios formos užsienio kišimosi prevenciją;

3° svarbiausius Prancūzijos ekonomikos, pramonės ir mokslo interesus;

4° teroristinių išpuolių prevenciją;

5° šių veiksmų prevenciją:
a) pasikėsinimų į respublikinę institucijų formą;
b) veiksmų, kuriais siekiama išlaikyti ar atkurti pagal L. 212-1 straipsnį išardytas grupuotes;
c) kolektyvinių smurto veiksmų, kurie gali labai pakenkti viešajai tvarkai;

6° nusikalstamumo ir organizuoto nusikalstamumo prevenciją;

7° masinio naikinimo ginklų platinimo prevenciją.“

33 CSI L. 811-4 straipsnyje nustatyta:

„*Conseil d'État* (Valstybės Taryba) dekretu, priimtu gavus *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija) nuomonę, nurodomos kitos nei specializuotos žvalgybos tarnybos, pavaldžios gynybos, vidaus ir teisingumo ministrams, taip pat už ekonomiką, biudžetą ar muitinę atsakingiems ministrams, kurioms gali būti leidžiama naudotis šios knygos V antraštinėje dalyje nurodytais būdais, laikantis toje pačioje knygoje nurodytų sąlygų. Jame kiekvienai tarnybai aiškiai nustatomi L. 811-3 straipsnyje nurodyti tikslai ir būdai, dėl kurių gali būti gautas leidimas.“

34 CSI L. 821-1 straipsnio pirmoje pastraipoje numatyta:

„Šios knygos V antraštinės dalies I–IV skyriuose nurodyti informacijos rinkimo būdai nacionalinėje teritorijoje gali būti įgyvendinami tik gavus išankstinį Ministro Pirmininko leidimą, kuris išduodamas gavus Nacionalinės žvalgybos būdų kontrolės komisijos nuomonę.“

35 CSI L. 821-2 straipsnyje numatyta:

„L. 821-1 straipsnyje nurodytas leidimas išduodamas gynybos ministrui, vidaus reikalų ministrui, teisingumo ministrui arba už ekonomiką, biudžetą ar muitinę atsakingam ministrui pateikus rašytinį ir motyvuotą prašymą. Kiekvienas ministras gali individualiai deleguoti šį įgaliojimą tik tiesiogiai su juo dirbantiems darbuotojams, turintiems teisę susipažinti su nacionalinio saugumo paslaptimi.

Prašyme nurodoma:

1° žvalgybos būdas ar būdai, kuris (-ie) bus taikomi;

2° tarnyba, dėl kurios teikiamas prašymas;

3° tikslas ar tikslai, kurių siekiama;

4° motyvas ar motyvai imtis priemonių;

5° leidimo galiojimo terminas;

6° duomenų subjektas ar subjektai, atitinkama vieta arba susijusios transporto priemonės.

Taikant 6 punktą asmenys, kurių tapatybė nežinoma, gali būti įvardyti pagal jų identifikatorius arba pagal jų statusą, o vietos arba transporto priemonės gali būti įvardytos nurodant asmenis, dėl kurių pateiktas prašymas.

<…>“

36 CSI L. 821-3 straipsnio pirmoje pastraipoje nurodyta:

„Prašymas pateikiamas *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija) pirmininkui arba, jeigu jo nėra, vienam iš komisijos narių, nurodytų L. 831-1 straipsnio 2 ir 3 punktuose, kurie per dvidešimt keturias valandas pateikia savo nuomonę Ministrui Pirmininkui. Jeigu prašymas nagrinėjamas ribotos ar visos sudėties komisijoje, apie tai nedelsiant pranešama Ministrui Pirmininkui ir nuomonė pateikiama per 72 valandas.“

37 CSI L. 821-4 straipsnyje numatyta:

„Ministras Pirmininkas išduoda leidimą taikyti šios knygos V antraštinės dalies I–IV skyriuose nurodytus būdus ne ilgesniam kaip keturių mėnesių laikotarpiui. <…> Leidime pateikiami motyvai ir L. 821-2 straipsnio 1–6 punktuose nurodyti reikalavimai. Bet kuris leidimas gali būti pratęstas tokiomis pačiomis sąlygomis, kokios numatytos šiame skyriuje.

Jeigu leidimas išduodamas po nepalankios *Commission nationale de contrôle des techniques de renseignement* (Nacionalinės žvalgybos būdų kontrolės komisija) nuomonės, jame nurodomi motyvai, dėl kurių tokios nuomonės nebuvo laikomasi.

<…>“

38 CSI L. 833-4 straipsnyje, esančiame šios antraštinės dalies III skyriuje, nustatyta:

„Savo iniciatyva arba gavusi bet kurio asmens, pageidaujančio patikrinti, ar jo atžvilgiu nėra neteisėtai naudojami žvalgybos būdai, skundą, komisija tikrina nurodytą žvalgybos būdą (-us), kad nustatytų, ar jie yra arba buvo taikomi laikantis šios knygos reikalavimų. Ji praneša skundą pateikusiam asmeniui, kad buvo atlikti būtini patikrinimai, tačiau nei patvirtina, nei paneigia, kad tie žvalgybos būdai buvo taikyti.“

39 CSI L. 841-1 straipsnio pirma ir antra pastraipos suformuluotos taip:

„Nepažeidžiant šio kodekso L. 854-9 straipsnyje numatytų specialių nuostatų, Valstybės Taryba, laikydamasi *Code de justice administrative* (Administracinio proceso kodeksas) VII knygos VII antraštinės dalies IIIa skyriuje nustatytų sąlygų, turi jurisdikciją nagrinėti skundus dėl šios knygos V antraštinėje dalyje nurodytų žvalgybos būdų įgyvendinimo.

Į ją gali kreiptis:

1° kiekvienas asmuo, pageidaujantis įsitikinti, ar jo atžvilgiu nėra neteisėtai naudojami žvalgybos būdai, ir galintis pateisinti išankstinį L. 833-4 straipsnyje numatytos procedūros taikymą;

2° *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija), laikydamasi L. 833-8 straipsnyje numatytų sąlygų.“

40 CSI įstatyminės dalies VIII knygos V antraštinėje dalyje dėl „informacijos rinkimo būdų, kuriems reikalingas leidimas“, be kita ko, yra I skyrius „Administracinės prieigos prie ryšio duomenų“, kuriame yra CSI L. 851-1–L. 851-7 straipsniai.

41 CSI L. 851-1 straipsnyje numatyta:

„Šios knygos II antraštinės dalies 1 skyriuje numatytomis sąlygomis gali būti leidžiama iš elektroninių ryšių operatorių ir asmenų, nurodytų [CPCE] L. 34-1 straipsnyje, taip pat asmenų, nurodytų *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (2004 m. birželio 21 d. Įstatymas Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika stiprinimo [JORF, 2004 m. birželio

22 d., p. 11168]) 6 straipsnio I dalies 1 ir 2 punktuose, rinkti informaciją ar dokumentus, tvarkomus ar saugomus jų tinkluose arba jiems teikiant elektroninių ryšių paslaugas, įskaitant techninius duomenis, susijusius su abonento numerių identifikavimu ar prisijungimu prie elektroninių ryšių paslaugų, su nurodyto asmens prisijungimo ar abonento numerių nustatymu, naudotų galinių įrenginių vietos nustatymu ir abonento komunikacijomis, t. y. numeriais, kuriais skambinta ir iš kurių gauti skambučiai, ryšio trukme ir data.

Nukrypstant nuo L. 821-2 straipsnio, individualiai paskirti ir įgalioti žvalgybos tarnybų, nurodytų L. 811-2 ir L. 811-4 straipsniuose, pareigūnai tiesiogiai perduoda *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija) rašytinius ir motyvuotus prašymus dėl techninių duomenų, susijusių su abonemento numerių identifikavimu ar prisijungimu prie elektroninių ryšių paslaugų arba su visų atitinkamo asmens abonentų numerių ar prisijungimų nustatymu. *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija), laikydamasi L. 821-3 straipsnyje numatytų sąlygų, pateikia savo nuomonę.

Ministro Pirmininko tarnyba yra atsakinga už informacijos ar dokumentų rinkimą iš operatorių ir asmenų, nurodytų šio straipsnio pirmoje pastraipoje. *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija) turi nuolatinę, visišką, tiesioginę ir greitą prieigą prie surinktos informacijos ir dokumentų.

Šio straipsnio taikymo tvarka nustatoma *Conseil d'État* (Valstybės Taryba) dekretu, priimtu gavus *Commission nationale de l'informatique et des libertés* (Nacionalinė informatikos ir laisvių komisija) bei *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija) nuomones."

42 CSI L. 851-2 straipsnyje nustatyta:

„I. Šios knygos II antraštinės dalies I skyriuje nustatytomis sąlygomis ir tik terorizmo prevencijos tikslais gali būti individualiai leidžiama realiuoju laiku rinkti L. 851-1 straipsnyje nurodytų operatorių ir asmenų tinkluose esančią informaciją ar dokumentus, nurodytus tame pačiame L. 851-1 straipsnyje, apie iš anksto identifikuotą asmenį, kuris gali būti susijęs su grėsme. Kai yra rimtų priežasčių manyti, kad vienas ar keli asmenys, susiję su asmens, dėl kurio išduotas leidimas, aplinka, gali pateikti informaciją dėl tikslo, kuriuo remiantis išduotas leidimas, toks leidimas gali būti išduodamas individualiai dėl kiekvieno iš šių asmenų.

Ia. Maksimalų leidimų, vienu metu išduotų pagal šį galiojantį straipsnį, skaičių nustato Ministras Pirmininkas, gavęs *Commission nationale de contrôle des techniques de renseignement* (Nacionalinė žvalgybos būdų kontrolės komisija) nuomonę. Komisijai pranešama apie sprendimą, kuriuo nustatoma ši kvota ir jos paskirstymas tarp L. 821-2 straipsnio pirmoje pastraipoje nurodytų ministrų, ir apie išduotų leidimų perimti informaciją skaičių.

<…>"

43 CPI L. 851-3 straipsnyje numatyta:

„I. Šios knygos II antraštinės dalies I skyriuje nustatytomis sąlygomis ir tik terorizmo prevencijos tikslais galima reikalauti, kad operatoriai ir L. 851-1 straipsnyje nurodyti asmenys savo tinkluose automatizuotai tvarkytų duomenis tam, kad, atsižvelgiant į leidime nurodytus parametrus, būtų nustatyti prisijungimai, galintys kelti terorizmo grėsmę.

Atliekant automatizuotą tvarkymą naudojama tik L. 851-1 straipsnyje nurodyta informacija ar dokumentai; kiti duomenys nei tie, kurie atitinka parametrus, nėra renkami ir neleidžiama nustatyti asmenų, su kuriais susijusi informacija ar dokumentai, tapatybės.

Laikantis proporcingumo principo, Ministro Pirmininko leidime patikslinama tokio tvarkymo techninė taikymo sritis.

II. Nacionalinė žvalgybos būdų kontrolės komisija pateikia nuomonę dėl prašymo išduoti leidimą dėl automatizuoto tvarkymo ir nustatytų aptikimo parametrų. Ji turi nuolatinę, visišką ir tiesioginę prieigą prie tokio tvarkymo ir surinktos informacijos bei duomenų. Ji yra informuojama apie visus tvarkymo ir parametrų pakeitimus ir gali teikti rekomendacijas.

Pirmasis leidimas atlikti automatizuotą tvarkymą, kaip numatyta šio straipsnio I dalyje, išduodamas dviem mėnesiams. Leidimas gali būti pratęstas laikantis šios knygos II antraštinės dalies I skyriuje nustatytų trukmės reikalavimų. Prašyme pratęsti leidimo galiojimo terminą pateikiama identifikatorių, apie kuriuos pranešta naudojant automatizuotą tvarkymą, skaičiaus nuoroda ir šių pranešimų reikšmingumo analizė.

III. L. 871-6 straipsnyje nustatytos sąlygos taikomos fizinėms operacijoms, kurias vykdo L. 851-1 straipsnyje nurodyti operatoriai ir asmenys.

IV. Kai šio straipsnio I dalyje nurodytas tvarkymas atskleidžia duomenis, galinčius rodyti teroristinio pobūdžio grėsmę, Ministras Pirmininkas arba vienas iš jo įgaliotų asmenų, gavęs Nacionalinės žvalgybos būdų kontrolės komisijos nuomonę, šios knygos II antraštinės dalies I skyriuje numatytomis sąlygomis gali leisti nustatyti atitinkamo asmens ar asmenų tapatybes ir surinkti su tuo susijusius duomenis. Šie duomenys panaudojami per 60 dienų nuo tokio surinkimo, o pasibaigus šiam laikotarpiui sunaikinami, išskyrus atvejus, kai yra rimtų įrodymų, patvirtinančių teroristinę grėsmę, susijusią su vienu ar keliais atitinkamais asmenimis.

<…>“

44 CSI L. 851-4 straipsnis suformuluotas taip:

„Šios knygos II antraštinės dalies I skyriuje numatytomis sąlygomis operatoriai, gavę prašymą, gali tinkle rinkti L. 851-1 straipsnyje nurodytus naudojamų galinių įrenginių buvimo vietos nustatymo techninius duomenis ir realiuoju laiku perduoti juos Ministro Pirmininko tarnybai.“

45 CSI R. 851-5 straipsnyje, kuris yra šio kodekso norminėje dalyje, numatyta:

„I. L. 851-1 straipsnyje nurodyta informacija ar dokumentai, išskyrus susirašinėjimo ar informacijos, kuri buvo naršyta, turinį, yra:

1° informacija ar dokumentai, nurodyti [CPCE] R. 10-13, R. 10-14 straipsniuose ir [Dekreto Nr. 2011-219] 1 straipsnyje;

2° kiti techniniai duomenys, nei nurodytieji 1 punkte:

a) leidžiantys nustatyti galinių įrenginių buvimo vietą;

b) susiję su galinės įrangos prieiga prie tinklų ar visuomeninių elektroninių ryšių paslaugų internetu;

c) susiję su elektroninių ryšių perdavimu tinklais;

d) susiję su naudotojo tapatybės, prisijungimo, tinklo ar viešo paskelbimo internetu paslaugos nustatymu ir autentiškumo patvirtinimu;

e) susiję su galinės įrangos savybėmis ir jų programinės įrangos konfigūracijos duomenimis.

II. Remiantis L. 851-1 straipsniu gali būti renkama tik informacija ir dokumentai, nurodyti I dalies 1 punkte. Toks rinkimas vyksta ne realiuoju laiku.

I dalies 2 punkte nurodyta informacija gali būti renkama tik pagal L. 851-2 ir L. 851-3 straipsnius, laikantis šiuose straipsniuose nustatytų sąlygų ir apribojimų ir taikant R. 851-9 straipsnį.“

CPCE

46 CPCE L. 34-1 straipsnyje numatyta:

„I. Šis straipsnis taikomas asmens duomenų tvarkymui teikiant visuomenei elektroninių ryšių paslaugas; visų pirma jis taikomas tinklams, palaikantiems identifikavimo ir duomenų rinkimo įrenginius.

II. Elektroninių ryšių operatoriai, visų pirma asmenys, kurių veikla – teikti visuomenei ryšių paslaugas internetu, sunaikina arba nuasmenina visus srauto duomenis, nepažeisdami III, IV, V ir VI dalių nuostatų.

Subjektai, teikiantys visuomenei elektroninių ryšių paslaugas, laikydamiesi pirmesnės pastraipos nustato vidaus tvarką kompetentingų institucijų prašymams vykdyti.

Subjektai, kurie, vykdydami pagrindinę arba papildomą profesinę veiklą, teikia visuomenei prisijungimo paslaugas, leidžiančias naudojantis prieiga prie tinklo palaikyti ryšius internetu (net ir nemokamai), privalo vykdyti pagal šį straipsnį elektroninių ryšių operatoriams taikomas nuostatas.

III. Tam, kad būtų nustatytos, atskleistos nusikalstamos veikos arba *Code de la propriété intellectuelle* (Intelektinės nuosavybės kodeksas) L. 336-3 straipsnyje nustatytos pareigos neįvykdymas ir pradėtas baudžiamasis persekiojimas už jas, arba tam, kad būtų užkirstas kelias prieš duomenų tvarkymo automatizuotomis priemonėmis sistemas rengiamoms atakoms, numatytoms Baudžiamojo kodekso 323-1–323-3-1 straipsniuose, už kurias baudžiama pagal minėtus straipsnius, ir siekiant vienintelio tikslo – prireikus užtikrinti, kad teisminei institucijai, Intelektinės nuosavybės kodekso L. 331-12 straipsnyje nurodytai viešajai institucijai arba *Code de la défense* (Gynybos kodeksas) L. 2321-1 straipsnyje nurodytai nacionalinei informacinių sistemų saugumo institucijai būtų suteikta reikiamos informacijos, ne ilgiau kaip vieniems metams gali būti atidėtas operacijų, kuriomis siekiama sunaikinti arba nuasmeninti tam tikrų kategorijų techninius duomenis, vykdymas. *Conseil d'État* (Valstybės Taryba) dekrete, priimtame gavus *Commission nationale de l'informatique et des libertés* (Nacionalinė informatikos ir laisvių komisija) nuomonę, laikantis VI dalyje nurodytų apribojimų, nustatomos šios duomenų kategorijos ir duomenų saugojimo trukmė, atsižvelgiant į operatorių veiklą ir ryšių pobūdį, taip pat nustatytų specifinių operatorių patiriamų papildomų išlaidų, susijusių su valstybės prašymu operatorių teikiamomis paslaugomis, kompensavimo tvarka.

<…>

VI. III, IV ir V dalyse nustatytomis sąlygomis saugomi ir tvarkomi duomenys yra susiję tik su operatorių teikiamų paslaugų naudotojų tapatybės nustatymu, techninėmis operatorių užtikrinamų ryšių savybėmis ir galinių įrenginių vieta.

Duomenys niekada negali būti susiję su atitinkamos korespondencijos turiniu ar informacija, kuri naršoma bet kokia forma naudojantis tokiais elektroniniais ryšiais.

Duomenys saugomi ir tvarkomi laikantis *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (1978 m. sausio 6 d. Informatikos, rinkmenų ir laisvių įstatymas Nr. 78-17) nuostatų.

Operatoriai imasi visų priemonių, siekdami neleisti šiais duomenimis naudotis kitais tikslais, nei numatyti šiame straipsnyje.“

47 CPCE R. 10-13 straipsnis suformuluotas taip:

I. Pagal L. 34-1 straipsnio III dalį elektroninių ryšių operatoriai nusikalstamų veikų tyrimo, konstatavimo ir baudžiamojo persekiojimo už jas tikslais saugo:

a) informaciją, leidžiančią nustatyti naudotojo tapatybę;

b) duomenis apie naudojamus galinius ryšių įrenginius;

c) informaciją apie kiekvieno ryšio technines savybes, taip pat jo datą, laiką ir trukmę;

d) duomenis apie prašytas arba naudotas papildomas paslaugas ir jų teikėjus;

e) duomenis, leidžiančius nustatyti ryšių adresato (-ų) tapatybę.

II. Kiek tai susiję su telefonijos veikla, operatorius išsaugo II dalyje nurodytus duomenis, taip pat duomenis, leidžiančius nustatyti ryšio kilmę ir vietą.

III. Šiame straipsnyje nurodyti duomenys saugomi vienus metus nuo įrašymo dienos.

IV. Nustatytos specifinės operatorių patiriamos papildomos išlaidos, susijusios su šiame straipsnyje nurodytų kategorijų duomenų teikimu, kurio reikalauja teisminės institucijos, kompensuojamos Baudžiamojo proceso kodekso R. 213-1 straipsnyje nustatyta tvarka.“

48 CPCE L. 10-14 straipsnyje numatyta:

„I. Pagal L. 34-1 straipsnio IV dalį elektroninių ryšių operatoriams leidžiama sąskaitų išrašymo ir mokėjimo operacijų tikslais saugoti techninius duomenis, leidžiančius nustatyti naudotojo tapatybę, ir R. 10-13 straipsnio I dalies b, c ir d punktuose nurodytus duomenis.

II. Kai vykdoma telefonijos veikla, operatoriai, be I dalyje nurodytų duomenų, gali saugoti techninius duomenis, susijusius su ryšio vietos ir pranešimo gavėjo (-ų) tapatybės nustatymu, ir sąskaitoms išrašyti skirtus duomenis.

III. Šio straipsnio I ir II dalyse nurodyti duomenys gali būti saugomi tik tuo atveju, jeigu jie reikalingi sąskaitoms už suteiktas paslaugas išrašyti ir mokėjimams už jas. Jie turi būti saugomi tik tiek, kiek būtina šiam tikslui pasiekti, bet ne ilgiau kaip vienus metus.

IV. Tinklų ir įrenginių saugumo tikslais operatoriai gali ne ilgiau kaip tris mėnesius saugoti:

a) duomenis, leidžiančius nustatyti ryšio kilmę;

b) informaciją apie kiekvieno ryšio technines savybes, taip pat jo datą, laiką ir trukmę;

c) duomenis, leidžiančius nustatyti ryšių adresato (-ų) tapatybę;

d) duomenis apie prašytas arba naudotas papildomas paslaugas ir jų teikėjus.“

2004 m. birželio 21 d. Įstatymas Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika stiprinimo

49 *Loi* nº 2004-575, *du 21 juin 2004, pour la confiance dans l'économie numérique* (2004 m. birželio 21 d. Įstatymas Nr. 2004-575 dėl pasitikėjimo skaitmenine ekonomika stiprinimo, JORF, 2004 m. birželio 22 d., p. 11168, toliau – LCEN) 6 straipsnyje numatyta:

„I. 1. Asmenys, siūlantys prieigą prie viešai prieinamų elektroninių ryšių paslaugų internetu, informuoja savo abonentus apie tai, kad yra techninių priemonių, leidžiančių apriboti prieigą prie tam tikrų paslaugų arba jas pasirinkti, ir jiems pasiūlo bent vieną iš šių priemonių.

<…>

2. Fiziniams ar juridiniams asmenims, kurie, net ir nemokamai, teikdami visuomenei ryšių paslaugas internetu laiko šių paslaugų gavėjų pateiktus signalus, rašytinę medžiagą, vaizdo, garso ar bet kokio pobūdžio pranešimus, negali būti taikoma civilinė atsakomybė už šių paslaugų gavėjo veiklą ar jo prašymu laikomą informaciją, jeigu jie iš tikrųjų nežinojo apie duomenų neteisėtumą, faktus ir aplinkybes, dėl kurių atsirado šis neteisėtumas, arba jeigu nuo momento, kai sužinojo apie neteisėtumą, nedelsdami ėmėsi veiksmų, kad pašalintų tokius duomenis arba padarytų prieigą prie jų neįmanomą.

<…>

II. I dalies 1 ir 2 punktuose nurodyti asmenys laiko ir saugo duomenis, kad būtų galima nustatyti asmenų, kurie prisidėjo kuriant jų teikiamų paslaugų turinį ar dalį turinio, tapatybę.

Jie suteikia asmenims, kurie redaguoja viešojo ryšio paslaugą internetu, technines priemones, kad šie laikytųsi III dalyje numatytų tapatybės nustatymo sąlygų.

Teisminė institucija gali prašyti, kad I dalies 1 ir 2 punktuose nurodyti paslaugų teikėjai pateiktų pirmoje pastraipoje nurodytus duomenis.

Baudžiamojo kodekso 226-17, 226-21 ir 226-22 straipsnių nuostatos taikomos šių duomenų tvarkymui.

Valstybės Taryba dekrete, priimtame gavus Nacionalinės informatikos ir laisvių komisijos nuomonę, apibrėžia pirmoje pastraipoje nurodytus duomenis ir nustato jų saugojimo trukmę ir tvarką.

<…>“

Dekretas Nr. 2011-219

50 Dekreto Nr. 2011-219, priimto remiantis LCEN 6 straipsnio II dalies paskutine pastraipa, I skyriuje yra šio dekreto 1–4 straipsniai.

51 Dekreto Nr. 2011-219 1 straipsnyje nustatyta:

„[LCEN] 6 straipsnio II dalyje nurodyti duomenys, kuriuos pagal šią nuostatą turi saugoti asmenys, yra šie:

1° asmenims, nurodytiems to paties straipsnio I dalies 1 punkte, dėl kiekvieno jų abonento prisijungimo:

a) prisijungimo identifikatorius;

b) identifikatorius, kurį tokie asmenys skiria abonentui;

c) prisijungimo terminalo identifikatorius, kai jie turi prieigą prie jo;

d) prisijungimo data, pradžios ir pabaigos laikas;

e) abonento linijos ypatybės;

2° asmenims, nurodytiems to paties straipsnio I dalies 2 punkte, dėl kiekvienos sukūrimo operacijos:

a) prisijungimo, inicijavusio ryšį, identifikatorius;

b) identifikatorius, kurį informacinė sistema priskyrė operacijos turiniui;

c) protokolų, naudojamų prijungti prie paslaugos ir turiniui perduoti, tipai;

d) operacijos pobūdis;

e) operacijos data ir laikas;

f) identifikatorius, kurį naudoja operaciją vykdantis asmuo, kai jis suteikia tokį identifikatorių;

3° to paties straipsnio I dalies 1 ir 2 punktuose nurodytiems asmenims – informacija, kurią naudotojas pateikė, sudarydamas sutartį arba sukurdamas paskyrą:

a) tuo metu, kai sukuriama paskyra, šio prisijungimo identifikatorius;

b) vardas ir pavardė arba pavadinimas;

c) susiję pašto adresai;

d) vartojami pseudonimai;

e) elektroninio pašto arba susijusių paskyrų adresai;

f) telefono numeriai;

g) naujausias slaptažodis ir duomenys, leidžiantys jį patikrinti arba pakeisti;

4° to paties straipsnio I dalies 1 ir 2 punktuose nurodytiems asmenims, kai sutarties sudarymas arba paskyros sukūrimas yra mokami, su mokėjimu susijusi informacija dėl kiekvienos mokėjimo operacijos:

a) naudojamo mokėjimo tipas;

b) mokėjimo numeris;

c) suma;

d) sandorio data ir laikas;

3 ir 4 punktuose nurodyti duomenys turi būti saugomi tik tada, jei asmenys paprastai juos renka.“

52 Šio dekreto 2 straipsnis suformuluotas taip:

„Indėlis kuriant turinį apima operacijas, susijusias su:

a) pradiniu turinio kūrimu;

b) turinio ir duomenų, susijusių su turiniu, pakeitimais;

c) turinio pašalinimu.“

53 Šio dekreto 3 straipsnyje numatyta:

„1 straipsnyje nurodytų duomenų saugojimo trukmė yra vieni metai:

a) 1 ir 2 punktuose minimų duomenų atveju – nuo turinio sukūrimo dienos kiekvienai operacijai, kuria prisidedama prie turinio kūrimo, kaip nurodyta 2 straipsnyje;

b) 3 punkte nurodytų duomenų atveju – nuo sutarties nutraukimo arba paskyros uždarymo dienos;

c) 4 punkte nurodytų duomenų atveju – nuo sąskaitos faktūros išrašymo arba mokėjimo operacijos dienos, taikant kiekvienai sąskaitai faktūrai ar mokėjimo operacijai.“

Belgijos teisė

54 2016 m. gegužės 29 d. įstatymu buvo visų pirma iš dalies pakeistos *Loi du 13 juin 2005 relative aux communications électroniques* (2005 m. birželio 13 d. Įstatymas dėl elektroninių ryšių, *Moniteur belge*, 2005 m. birželio 20 d., p. 28070; toliau – 2005 m. birželio 13 d. įstatymas), *Code d'instruction criminelle* (Baudžiamojo proceso kodeksas, toliau – Baudžiamojo proceso kodeksas) ir *Loi du 30 novembre 1998 organique des services de renseignement et de sécurité* (1998 m. lapkričio 30 d. Pagrindų įstatymas dėl žvalgybos ir saugumo tarnybų, *Moniteur belge*, 1998 m. gruodžio 18 d., p. 40312; toliau – 1998 m. lapkričio 30 d. įstatymas) nuostatos.

55 2005 m. birželio 13 d. įstatymo, iš dalies pakeisto 2016 m. gegužės 29 d. įstatymu, 126 straipsnyje nustatyta:

„1. Nepažeidžiant *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (1992 m. gruodžio 8 d. Įstatymas dėl privataus gyvenimo apsaugos tvarkant asmens duomenis), telefonijos (įskaitant internetinę telefoniją), interneto prieigos ir interneto elektroninio pašto viešųjų paslaugų teikėjai, operatoriai, teikiantys viešai prieinamų elektroninių ryšių tinklų paslaugas, ir operatoriai, teikiantys vieną iš šių paslaugų, saugo 3 dalyje nurodytus duomenis, kuriuos jie generuoja ar tvarko, teikdami atitinkamas ryšių paslaugas.

Šis straipsnis netaikomas ryšių turiniui.

Šio straipsnio 3 dalyje nurodyta pareiga saugoti duomenis taikoma ir neatsakytiems skambučiams, jeigu teikiant atitinkamas ryšių paslaugas šiuos duomenis:

1° telefonijos duomenų atveju – generuoja arba tvarko viešai prieinamų elektroninių ryšių paslaugų arba viešųjų elektroninių ryšių tinklų operatoriai; arba

2° interneto duomenų atveju – užfiksavo šių paslaugų teikėjai.

2. Tik toliau išvardytos valdžios institucijos gali pateikusios prašymą 1 dalies pirmoje pastraipoje nurodytiems paslaugų teikėjams ir operatoriams gauti pagal šį straipsnį saugomus duomenis toliau išvardytais tikslais ir sąlygomis:

1° teisminės institucijos tam, kad būtų nustatytos nusikalstamos veikos, atliktas jų ikiteisminis tyrimas ir vykdomas persekiojimas dėl jų, siekiant įgyvendinti *Code d'instruction criminelle* (Baudžiamojo proceso kodeksas) 46a ir 88a straipsniuose numatytas priemones, šiuose straipsniuose numatytomis sąlygomis;

2° žvalgybos ir saugumo tarnybos tam, kad būtų įvykdytos žvalgybos užduotys naudojant duomenų rinkimo būdus, numatytus *Loi du 30 novembre 1998 organique des services de renseignement et de sécurité* (1998 m. lapkričio 30 d. Pagrindų įstatymas dėl žvalgybos ir saugumo tarnybų) 16/2, 18/7 ir 18/8 straipsniuose, ir laikantis tame įstatyme numatytų sąlygų;

3° bet kuris [*Institut belge des services postaux et des télécommunications* (Belgijos pašto ir telekomunikacijų paslaugų institutas)] kriminalinės policijos pareigūnas, siekdamas nustatyti 114, 124 straipsniuose ir šiame straipsnyje numatytas nusikalstamas veikas, atlikti jų ikiteisminį tyrimą ir vykdyti baudžiamąjį persekiojimą už jas;

4° skubios pagalbos tarnybos, teikiančios pagalbą įvykio vietoje, kai po pagalbos skambučio jos iš atitinkamo paslaugų teikėjo ar operatoriaus iš 107 straipsnio 2 dalies trečioje pastraipoje nurodytų duomenų bazių negauna skambintojo tapatybę leidžiančių nustatyti duomenų arba gauna neišsamius ar neteisingus duomenis. Galima prašyti tik skambintojo tapatybę leidžiančių nustatyti duomenų ir ne vėliau kaip per 24 valandas po skambučio;

5° *Cellule des personnes disparues de la Police Fédérale* (Federalinės policijos dingusių asmenų padalinys) kriminalinės policijos pareigūnas, vykdydamas pagalbos pavojuje atsidūrusiam asmeniui užduotį, ieškantis asmenų, kurių dingimas kelia susirūpinimą, ir jeigu yra svarių prielaidų ar požymių, kad dingusio asmens fiziniam neliečiamumui gresia tiesioginis pavojus. Per Karaliaus paskirtą policijos tarnybą galima iš atitinkamo operatoriaus ar paslaugų teikėjo prašyti tik 3 dalies pirmoje ir antroje pastraipose nurodytų duomenų, susijusių su dingusiu asmeniu ir saugomų 48 valandas iki prašymo pateikti duomenų gavimo;

6° *Service de médiation pour les télécommunications* (Tarpininkavimo sprendžiant telekomunikacijų ginčus tarnyba), siekdama identifikuoti asmenį, kuris piktavališkai naudojosi elektroninių ryšių tinklu ar paslauga, laikantis *Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques* (1991 m. kovo 21 d. Įstatymas dėl tam tikrų valstybės ūkio įmonių reformos) 43a straipsnio 3 dalies 7 punkte nustatytų sąlygų. Gali būti prašoma tik identifikavimo duomenų.

1 dalies pirmoje pastraipoje nurodyti paslaugų teikėjai ir operatoriai užtikrina, kad 3 dalyje nurodyti duomenys būtų neribotai pasiekiami iš Belgijos ir kad šiuos duomenis ir bet kurią kitą su jais susijusią būtiną informaciją būtų galima nedelsiant perduoti tik šioje dalyje nurodytoms institucijoms.

Nepažeidžiant kitų teisės nuostatų, 1 dalies pirmoje pastraipoje nurodyti paslaugų teikėjai ir operatoriai negali pagal 3 dalį saugomų duomenų naudoti kitais tikslais.

3. Duomenys, leidžiantys identifikuoti naudotoją ar abonentą ir ryšio priemones, išskyrus antroje ir trečioje pastraipose konkrečiai numatytus duomenis, saugomi dvylika mėnesių nuo tos dienos, kurią ryšys paskutinį kartą buvo įmanomas naudojantis atitinkama paslauga.

Duomenys, susiję su galinio įrenginio prieiga ir prijungimu prie tinklo ir paslaugų bei šios įrangos buvimo vieta, įskaitant tinklo galinį tašką, saugomi dvylika mėnesių nuo ryšio datos.

Ryšio duomenys, įskaitant jų siuntėją ir adresatą, išskyrus turinį, saugomi dvylika mėnesių nuo ryšio datos.

Conseil des ministres (Ministrų Taryba) apsvarstytame nutarime Karalius, remdamasis teisingumo ministro ir ministro [atsakingo už elektroninių ryšių sritį] pasiūlymu, *Commission de la protection de la vie privée* (Privatumo apsaugos komisija) ir Institutui pateikus nuomonę, nustato saugotinus duomenis, suskirstytus į pirmoje–trečioje pastraipose nurodytas kategorijas, ir reikalavimus, kuriuos šie duomenys turi atitikti.

<…>“

Pagrindinės bylos ir prejudiciniai klausimai

Byla C-511/18

56 2015 m. lapkričio 30 d. ir 2016 m. kovo 16 d. prašymais, kurie buvo prijungti prie pagrindinės bylos, *Quadrature du Net*, *French Data Network* ir *Fédération des fournisseurs d’accès à Internet associatifs* (Asocijuotųjų prieigos prie interneto teikėjų federacija), taip pat *Igwan.net* pateikė skundus *Conseil d’État* (Valstybės Taryba, Prancūzija), juose prašo panaikinti dekretus Nr. 2015-1185, 2015-1211, 2015-1639 ir 2016-67, motyvuodami, be kita ko, tuo, kad jais pažeidžiama Prancūzijos Konstitucija, Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (toliau – EŽTK), taip pat direktyvos 2000/31 ir 2002/58, siejamos su Chartijos 7, 8 ir 47 straipsniais.

57 Konkrečiai dėl pagrindų, grindžiamų Direktyvos 2000/31 pažeidimu, prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, kad pagal CSI L. 851-3 straipsnio nuostatas elektroninių ryšių operatoriai ir techniniai paslaugų teikėjai įpareigojami „savo tinkluose automatizuotai tvarkyt[i] duomenis tam, kad, atsižvelgiant į leidime nurodytus parametrus, būtų nustatyti prisijungimai, galintys kelti terorizmo grėsmę“. Šis būdas skirtas tik ribotą laiką iš šių operatorių ir paslaugų teikėjų visų tvarkomų ryšio duomenų gauti duomenims, kurie galėtų būti susiję su tokiu sunkiu nusikaltimu. Šiomis aplinkybėmis minėtomis nuostatomis, kuriose nenustatyta bendra aktyvaus stebėjimo pareiga, nepažeidžiamas Direktyvos 2000/31 15 straipsnis.

58 Dėl pagrindų, grindžiamų Direktyvos 2002/58 pažeidimu, prašymą priimti prejudicinį sprendimą pateikęs teismas teigia, kad visų pirma iš šios direktyvos nuostatų bei 2016 m. gruodžio 21 d. Sprendimo *Tele2 Sverige ir Watson ir kt.* (C-203/15 ir C-698/15, EU:C:2016:970 toliau – Sprendimas *Tele2*) matyti, kad nacionalinės teisės nuostatos, kuriose nustatytos pareigos elektroninių ryšių paslaugų teikėjams, kaip antai bendrai ir nediferencijuojant saugoti srauto ir naudotojų bei abonentų vietos nustatymo duomenis minėtos direktyvos 15 straipsnio 1 dalyje numatytais tikslais, tarp kurių yra ir nacionalinio saugumo apsauga, gynyba ir visuomenės saugumas, patenka į šios direktyvos taikymo sritį tiek, kiek jos reglamentuoja minėtų paslaugų teikėjų veiklą. Tas pats pasakytina apie nacionalinės teisės nuostatas, reglamentuojančias nacionalinės valdžios institucijų prieigą prie duomenų ir jų naudojimą.

59 Prašymą priimti prejudicinį sprendimą pateikęs teismas iš to daro išvadą, kad į Direktyvos 2002/58 taikymo sritį patenka tiek iš CSI L. 851-1 straipsnio kylanti pareiga saugoti duomenis, tiek minėto kodekso L. 851-1, L. 851-2 ir L. 851-4 straipsniuose numatyta administracinė prieiga prie šių duomenų, įskaitant prieigą realiuoju laiku. To teismo teigimu, tas pats pasakytina ir apie to paties kodekso L. 851-3 straipsnio nuostatas, kurios, nors nenustato atitinkamiems operatoriams bendros duomenų saugojimo pareigos, juos vis dėlto įpareigoja savo tinkluose įgyvendinti automatizuotą tvarkymą, skirtą identifikuoti prisijungimams, galintiems kelti terorizmo grėsmę.

60 Vis dėlto tas teismas mano, kad į Direktyvos 2002/58 taikymo sritį nepatenka CSI nuostatos, nurodytos prašymuose dėl panaikinimo, kurios yra susijusios su valstybės tiesiogiai įgyvendinamais informacijos rinkimo būdais, nereglamentuojant elektroninių ryšių paslaugų teikėjų veiklos ir jiems nenustatant konkrečių pareigų. Taigi šios nuostatos negali būti laikomos įgyvendinančiomis Sąjungos teisę, todėl negalima veiksmingai remtis pagrindais, grindžiamais tuo, kad šiomis nuostatomis pažeidžiama Direktyva 2002/58.

61 Taigi, siekiant išspręsti ginčus, susijusius su dekretų Nr. 2015-1185, 2015-1211, 2015-1639 ir 2016-67 teisėtumu Direktyvos 2002/58 atžvilgiu, kiek jie buvo priimti įgyvendinant CSI L. 851-1–L. 851-4 straipsnius, kyla trys Sąjungos teisės aiškinimo klausimai.

62 Kiek tai susiję su Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimu, prašymą priimti prejudicinį sprendimą pateikusiam teismui kyla klausimas, pirma, ar, atsižvelgiant į administracinės prieigos prie ryšio duomenų bei jų naudojimo garantijas ir kontrolę, elektroninių ryšių paslaugų teikėjams pagal CSI L. 851-1 ir R. 851-5 straipsnius nustatyta pareiga bendrai ir nediferencijuotai saugoti duomenis turi būti laikoma suvaržymu, pateisinamu pagal Chartijos 6 straipsnį užtikrinama teise į saugumą ir nacionalinio saugumo reikalavimais, už kuriuos atsakomybė pagal ESS 4 straipsnį tenka tik valstybėms narėms.

63 Antra, dėl kitų įpareigojimų, kurie gali būti nustatyti elektroninių ryšių paslaugų teikėjams, prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, kad pagal CSI L. 851-2 straipsnio nuostatas tik terorizmo prevencijos tikslais leidžiama iš tų pačių asmenų rinkti informaciją ar dokumentus, numatytus šio kodekso L. 851-1 straipsnyje. Šis duomenų rinkimas, susijęs tik su vienu ar keliais asmenimis, kurie prieš tai identifikuoti kaip keliantys terorizmo grėsmę, vyksta realiuoju laiku. Tas pats pasakytina apie minėto kodekso L. 851-4 straipsnio nuostatas, pagal kurias operatoriams leidžiama realiuoju laiku perduoti tik techninius duomenis apie galinių įrenginių vietą. Šie būdai taikomi tokiais tikslais ir tvarka, kurie skiriasi nuo administracinės prieigos prie pagal CPCE ir LCEN saugomų duomenų realiuoju laiku, atitinkamiems teikėjams nenustatant papildomo reikalavimo saugoti duomenis, palyginti su tuo, kas būtina sąskaitoms išrašyti ir jų paslaugoms teikti. Be to, CSI L. 851-3 straipsnio nuostatomis, kuriose numatyta paslaugų teikėjų pareiga savo tinkluose atlikti automatizuotą prisijungimų analizę, taip pat nenustatomas bendro ir nediferencijuoto duomenų saugojimo reikalavimas.

64 Prašymą priimti prejudicinį sprendimą pateikęs teismas mano, kad tiek bendras ir nediferencijuotas duomenų saugojimas, tiek prieiga prie prisijungimo duomenų realiuoju laiku teikia analogų neturinčią operatyvinę naudą, atsižvelgiant į didelę ir nuolatinę grėsmę nacionaliniam saugumui, ypač susijusią su terorizmo rizika. Iš tiesų bendras ir nediferencijuotas duomenų saugojimas leidžia žvalgybos tarnyboms gauti prieigą prie ryšių duomenų prieš nustatant priežastis, dėl kurių atitinkamas asmuo būtų laikomas keliančiu grėsmę visuomenės saugumui, gynybai ar valstybės saugumui. Be to, prieiga prie ryšio duomenų realiuoju laiku leidžia sparčiai reaguojant sekti asmenų, kurie gali nedelsiant kelti grėsmę viešajai tvarkai, elgesį.

65 Taip pat CSI L. 851-3 straipsnyje numatytas būdas leidžia, remiantis šiuo tikslu konkrečiai apibrėžtais kriterijais, nustatyti asmenis, kurių elgesys, atsižvelgiant į jų komunikavimo būdus, gali kelti terorizmo grėsmę.

66 Trečia, kiek tai susiję su kompetentingų institucijų prieiga prie saugomų duomenų, prašymą priimti prejudicinį sprendimą pateikęs teismas siekia išsiaiškinti, ar Direktyva 2002/58, siejama su Chartija, turi būti aiškinama taip, kad pagal ją visais atvejais ryšio duomenų rinkimo procedūrų teisėtumas siejamas su atitinkamų asmenų informavimo reikalavimu, kai tokia informacija nebegali pakenkti kompetentingų institucijų atliekamiems tyrimams, ar tokios procedūros gali būti laikomos teisėtomis, atsižvelgiant į visas kitas nacionalinėje teisėje numatytas procesines garantijas, kai jomis užtikrinama teisė į veiksmingą teisinę gynybą.

67 Dėl šių kitų procesinių garantijų prašymą priimti prejudicinį sprendimą pateikęs teismas, be kita ko, patikslina, kad bet kuris asmuo, norintis patikrinti, ar jo atžvilgiu nėra neteisėtai naudojami žvalgybos būdai, gali kreiptis į specialią *Conseil d'État* (Valstybės Taryba) kolegiją, kuri, atsižvelgdama į informaciją, jai pateiktą per kitą nei rungimosi principu grindžiamą procesą, turi patikrinti, ar pareiškėjui taikytas žvalgybos būdas ir ar jis buvo įgyvendintas laikantis CSI VIII knygos. Šiai kolegijai suteikti įgaliojimai nagrinėti prašymus užtikrina jos vykdomos teisminės kontrolės veiksmingumą. Taigi ji turi kompetenciją nagrinėti prašymus, savo iniciatyva tirti visus nustatytus pažeidimus ir nurodyti administracijai imtis visų reikalingų priemonių konstatuotiems pažeidimams pašalinti. Be to, Nacionalinė žvalgybos būdų kontrolės komisija turi patikrinti, ar informacijos rinkimo būdai nacionalinėje teritorijoje yra taikomi laikantis CSI reikalavimų. Taigi aplinkybė, kad pagrindinėje byloje nagrinėjamose teisės aktų nuostatose nenumatyta, jog suinteresuotiesiems asmenims turi būti pranešta apie jiems taikomas stebėjimo priemones, savaime nėra per didelis teisės į privataus gyvenimą apribojimas.

68 Šiomis aplinkybėmis Valstybės Taryba nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar tokiomis aplinkybėmis, kai nacionaliniam saugumui keliama didelė nuolatinė grėsmė, ypač susijusi su terorizmo pavojumi, pagal [Direktyvos 2002/58] 15 straipsnio 1 dalies leidžiančiąsias nuostatas paslaugų teikėjams numatyta pareiga bendrai ir nediferencijuojant saugoti duomenis turi būti laikoma teisių suvaržymu, pateisinamu pagal [Chartijos] 6 straipsnį užtikrinama teise į saugumą ir nacionalinio saugumo reikalavimais, už kuriuos atsakomybė pagal [ESS] 4 straipsnį tenka tik valstybėms narėms?

2. Ar [Direktyva 2002/58], siejama su [Chartija], turi būti aiškinama taip, kad ja leidžiamos teisėkūros priemonės, kaip antai skirtos rinkti srauto ir konkrečių asmenų vietos nustatymo duomenims realiu laiku, kurios, nors ir daro poveikį elektroninių ryšių paslaugų teikėjų teisėms ir pareigoms, vis dėlto nenustato konkrečios jų duomenų saugojimo pareigos?

3. Ar [Direktyva 2002/58], siejama su [Chartija], turi būti aiškinama taip, jog tam, kad prisijungimo duomenų rinkimas būtų teisėtas, pagal ją visais atvejais taikomas reikalavimas apie tai informuoti duomenų subjektus, kai toks informavimas nebegali neigiamai paveikti kompetentingų institucijų atliekamų tyrimų, ar toks rinkimas taip pat gali būti laikomas teisėtu atsižvelgiant į visas kitas egzistuojančias procesines garantijas, jeigu jomis užtikrinama teisė į veiksmingą teisinę gynybą?“

Byla C-512/18

69 2015 m. rugsėjo 1 d. *French Data Network*, *la Quadrature du Net* ir *Fédération des fournisseurs d'accès à Internet associatifs* pateikė *Conseil d'État* (Valstybės Taryba) skundą, juo prašė panaikinti dėl Ministro Pirmininko atsakymo nepateikimo implicitinį sprendimą atmesti jų prašymą panaikinti CPCE R. 10-13 straipsnį ir Dekretą Nr. 2011-219 dėl to, kad, be kita ko, šiais teisės aktais pažeidžiama Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais. *Privacy International* ir *Center for Democracy and Technology* buvo leista įstoti į pagrindinę bylą.

70 Dėl CPCE R. 10-13 straipsnio ir jame numatytos pareigos bendrai ir nediferencijuotai saugoti ryšių duomenis prašymą priimti prejudicinį sprendimą pateikęs teismas, kuris pateikia argumentų, panašių į pateiktus byloje C-511/18, pažymi, kad toks saugojimas leidžia teisminei institucijai susipažinti su asmens ryšių duomenimis prieš jį įtariant padarius nusikalstamą veiką, todėl toks saugojimas teikia analogų neturinčią naudą nusikalstamų veikų ištyrimui, nustatymui ir baudžiamajam persekiojimui už jas.

71 Kiek tai susiję su Dekretu Nr. 2011-219, prašymą priimti prejudicinį sprendimą pateikęs teismas teigia, kad LCEN 6 straipsnio II dalis, kurioje nustatyta pareiga laikyti ir saugoti tik tuos duomenis, kurie susiję su turinio sukūrimu, patenka ne į Direktyvos 2002/58 taikymo sritį, nes pagal jos 3 straipsnio 1 dalį ji apima tik viešai prieinamų elektroninių ryšių paslaugų teikimą viešais ryšių tinklais Sąjungoje, bet į Direktyvos 2000/31 taikymo sritį.

72 Vis dėlto tas teismas mano, kad iš Direktyvos 2000/31 15 straipsnio 1 ir 2 dalių matyti, jog joje nenustatytas principinis draudimas saugoti duomenis, susijusius su turinio kūrimu, nuo kurio būtų galima nukrypti tik taikant išimtį. Taigi kyla klausimas, ar minėtos direktyvos 12, 14 ir 15 straipsniai, siejami su Chartijos 6–8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinami taip, kad pagal juos valstybei narei leidžiama priimti nacionalinės teisės aktus, kaip antai LCEN 6 straipsnio II dalį, pagal kuriuos atitinkami asmenys įpareigojami saugoti duomenis, leidžiančius nustatyti asmenis, dalyvavusius kuriant jų teikiamų paslaugų turinį, kad prireikus teisminė institucija galėtų iš jų pareikalauti perduoti šiuos duomenis, siekdama užtikrinti, kad būtų laikomasi civilinę ar baudžiamąją atsakomybę reglamentuojančių nuostatų.

73 Šiomis aplinkybėmis *Conseil d'État* (Valstybės Taryba) nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui šiuos prejudicinius klausimus:

„1. Ar pagal [Direktyvos 2002/58] 15 straipsnio 1 dalies leidžiančiąsias nuostatas paslaugų teikėjams numatyta pareiga bendrai ir nediferencijuojant saugoti duomenis turi būti laikoma, ypač atsižvelgiant į garantijas ir kontrolę, kurios vėliau taikytinos šių prisijungimo duomenų rinkimui ir jų naudojimui, teisių suvaržymu, pateisinamu pagal [Chartijos] 6 straipsnį užtikrinama teise į saugumą ir nacionalinio saugumo reikalavimais, dėl kurių atsakomybė pagal [ESS] 4 straipsnį tenka tik valstybėms narėms?

2. Ar Direktyvos [2000/31] nuostatos, atsižvelgiant į [Chartijos] 6, 7, 8 ir 11 straipsnius bei 52 straipsnio 1 dalį, turi būti aiškinamos taip, kad jomis leidžiama valstybei narei nustatyti nacionalinį reglamentavimą, pagal kurį asmenys, kurių veikla yra teikti visuomenei ryšio paslaugas internetu, ir fiziniai ar juridiniai asmenys, kurie užtikrina, net ir nemokamai, teikiant visuomenei ryšių paslaugas internetu šių paslaugų gavėjų pateiktų signalų, rašytinės medžiagos, vaizdo, garso ar bet kokio pobūdžio pranešimų saugojimą, būtų įpareigoti saugoti duomenis, leidžiančius nustatyti asmenų, dalyvavusių kuriant jų teikiamų paslaugų turinį, tapatybę, kad prireikus teisminė institucija galėtų iš jų pareikalauti perduoti šiuos duomenis, siekdama užtikrinti, kad būtų laikomasi civilinę ar baudžiamąją atsakomybę reglamentuojančių nuostatų?“

Byla C-520/18

74 2017 m. sausio 10 d., sausio 16 d., sausio 17 d. ir sausio 18 d. pateiktais prašymais, kurie buvo sujungti pagrindinėje byloje, *Ordre des barreaux francophones et germanophone*, *Académie Fiscale ASBL*, UA, *Liga voor Mensenrechten ASBL*, *Ligue des Droits de l'Homme ASBL*, VZ, WY ir WW kreipėsi į *Cour constitutionnelle* (Konstitucinis Teismas, Belgija), prašydami panaikinti 2016 m. gegužės 29 d. įstatymą, remdamiesi tuo, kad šiuo įstatymu pažeidžiami Belgijos Konstitucijos 10 ir 11 straipsniai, siejami su EŽTK 5, 6–11, 14, 15, 17 ir 18 straipsniais, Chartijos 7, 8, 11, 47 straipsniai ir 52 straipsnio 1 dalis, Tarptautinio pilietinių ir politinių teisių pakto, kurį Jungtinių Tautų Generalinė asamblėja priėmė 1966 m. gruodžio 16 d. ir kuris įsigaliojo 1976 m. kovo 23 d., 17 straipsnis, bendrieji teisinio saugumo, proporcingumo ir informacinio apsisprendimo principai bei ESS 5 straipsnio 4 dalis.

75 Grįsdami savo prašymus pareiškėjai pagrindinėje byloje iš esmės teigia, kad 2016 m. gegužės 29 d. įstatymo neteisėtumas visų pirma susijęs su tuo, kad juo viršijama tai, kas griežtai būtina, ir jame nenumatyta pakankamų apsaugos garantijų. Visų pirma nei jo nuostatos, susijusios su duomenų saugojimu, nei nuostatos, reglamentuojančios valdžios institucijų prieigą prie saugomų duomenų, neatitinka reikalavimų, nustatytų 2014 m. balandžio 8 d. Sprendime *Digital Rights Ireland ir kt.*

(C-293/12 ir C-594/12, EU:C:2014:238, toliau – Sprendimas *Digital Rights*) ir 2016 m. gruodžio 21 d. Sprendime *Tele2* (C-203/15 ir C-698/15, EU:C:2016:970). Iš tiesų šiomis nuostatomis keliamas pavojus, kad bus nustatyti asmeniniai profiliai, kuriais kompetentingos institucijos gali piktnaudžiauti, jose taip pat nenumatytas tinkamas saugomų duomenų saugumo ir apsaugos lygis. Galiausiai šis įstatymas taikomas asmenims, kuriems taikomas profesinės paslapties reikalavimas, ir asmenims, turintiems konfidencialumo pareigą, ir yra susijęs su jautriais ryšių asmens duomenimis, nenumatant specialių garantijų siekiant apsaugoti tokius duomenis.

76 Prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, kad duomenys, kuriuos pagal 2016 m. gegužės 29 d. įstatymą turi saugoti telefonijos paslaugų, įskaitant teikiamas internetu, interneto prieigos ir elektroninio pašto paslaugų teikėjai ir operatoriai, teikiantys viešuosius elektroninių ryšių tinklus, yra identiški nurodytiems 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyvoje 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičiančioje Direktyvą 2002/58/EB (OL L 105, 2006, p. 54), nediferencijuojant pagal duomenų subjektus ar siekiamą tikslą. Šiuo klausimu tas teismas patikslina, kad šiuo įstatymu teisės aktų leidėjo siekiamas tikslas yra ne tik kovoti su terorizmu ir vaikų pornografija, bet ir turėti galimybę naudoti saugomus duomenis įvairiose situacijose, kai vyksta baudžiamasis tyrimas. Be to, prašymą priimti prejudicinį sprendimą pateikęs teismas konstatuoja, kad iš minėto įstatymo aiškinamojo memorandumo matyti, jog nacionalinės teisės aktų leidėjas manė, kad, atsižvelgiant į siekiamą tikslą, neįmanoma nustatyti tikslinio ir diferencijuoto saugojimo pareigos ir kad jis nusprendė bendro ir nediferencijuoto saugojimo pareigai taikyti griežtas garantijas, kiek tai susiję tiek su saugomais duomenimis, tiek su prieiga prie jų, kad būtų kiek įmanoma apibrėžtas teisės į privataus gyvenimą suvaržymas.

77 Prašymą priimti prejudicinį sprendimą pateikęs teismas priduria, kad 2005 m. birželio 13 d. įstatymo redakcijos, pakeistos 2016 m. gegužės 29 d. įstatymu, 126 straipsnio 2 dalies 1 ir 2 punktuose numatytos sąlygos, kuriomis atitinkamai teisminės ir žvalgybos bei saugumo tarnybos gali gauti prieigą prie saugomų duomenų, todėl šio įstatymo teisėtumo, atsižvelgiant į Sąjungos teisės reikalavimus, nagrinėjimas turėtų būti sustabdytas, kol Teisingumo Teismas priims sprendimus dviejose jo nagrinėjamose prejudicinėse bylose, susijusiose su tokia prieiga.

78 Galiausiai prašymą priimti prejudicinį sprendimą pateikęs teismas pažymi, kad 2016 m. gegužės 29 d. įstatymu siekiama sudaryti sąlygas veiksmingai vykdyti baudžiamąjį tyrimą ir taikyti veiksmingas sankcijas, kiek tai susiję su nepilnamečių seksualiniu išnaudojimu, taip pat nustatyti tokį nusikaltimą padariusio asmens tapatybę, net kai jis naudojasi elektroninių ryšių priemonėmis. Per tame teisme vykusį procesą šiuo klausimu buvo atkreiptas dėmesys į pareigas veikti, kylančias iš EŽTK 3 ir 8 straipsnių. Šios pareigos taip pat gali kilti iš atitinkamų Chartijos nuostatų, galinčių turėti įtakos Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimui.

79 Tokiomis aplinkybėmis *Cour constitutionnelle* (Konstitucinis Teismas) nusprendė sustabdyti bylos nagrinėjimą ir pateikti Teisingumo Teismui tokius prejudicinius klausimus:

„1. Ar Direktyvos [2002/58] 15 straipsnio 1 dalį, siejamą su teise į saugumą, garantuojama [Chartijos] 6 straipsniu, ir teise į asmens duomenų apsaugą, garantuojama [Chartijos] 7, 8 straipsniais ir 52 straipsnio 1 dalimi, reikia aiškinti taip, kad pagal ją draudžiamos tokios nacionalinės teisės nuostatos, kokios yra nagrinėjamos, kuriose numatyta bendra operatorių ir elektroninių ryšių paslaugų teikėjų pareiga saugoti srauto ir vietos nustatymo duomenis, kaip jie suprantami pagal Direktyvą [2002/58], jų generuojamus ar tvarkomus teikiant šias paslaugas, t. y. nacionalinės teisės nuostatos, kurių tikslas yra ne vien sunkių nusikaltimų tyrimas, nustatymas ar persekiojimas už juos, bet ir nacionalinio saugumo, teritorijos gynybos ir viešojo saugumo užtikrinimas, kitų nei sunkūs nusikaltimai veikų tyrimas, nustatymas ir persekiojimas už jas ar draudžiamo elektroninių ryšių sistemų naudojimo prevencija ar kito tikslo, nurodyto Reglamento [2016/679] 23 straipsnio 1 dalyje, siekimas, kai šiose teisės nuostatose taip pat numatytos garantijos, susijusios su duomenų saugojimu ir prieiga prie jų?

2. Ar Direktyvos [2002/58] 15 straipsnio 1 dalį, siejamą su [Chartijos] 4, 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, reikia aiškinti taip, kad pagal ją draudžiamos tokios nacionalinės teisės nuostatos, kokios yra nagrinėjamos, kuriose numatyta bendra operatorių ir elektroninių ryšių paslaugų teikėjų pareiga saugoti srauto ir vietos nustatymo duomenis, kaip jie suprantami pagal Direktyvą [2002/58], jų generuojamus ar tvarkomus teikiant šias paslaugas, jeigu šių nacionalinės teisės nuostatų tikslas, be kita ko, yra padėti valdžios institucijoms vykdyti pagal Chartijos 4 ir [7] straipsnius joms tenkančias pareigas veikti, pagal kurias turi būti nustatytas teisinis pagrindas, kuris sudarytų sąlygas veiksmingam nusikalstamos veikos tyrimui ir veiksmingam nubaudimui už nepilnamečių seksualinį išnaudojimą ir kuris faktiškai leistų identifikuoti nusikalstamą veiką padariusį asmenį ir tuomet, kai naudotasi elektroninių ryšių priemonėmis?

3. Ar tuo atveju, jeigu remdamasis atsakymais į pirmąjį ir antrąjį prejudicinius klausimus *Cour constitutionnelle* (Konstitucinis Teismas) padarytų išvadą, kad ginčijamu įstatymu pažeidžiamas vienas ar keli įsipareigojimai pagal šiuose klausimuose nurodytas nuostatas, jis galėtų laikinai palikti galioti [2016 m. gegužės 29 d. įstatymą], kad būtų išvengta teisinio nesaugumo ir anksčiau surinkti bei saugomi duomenys dar galėtų būti panaudoti įstatyme numatytais tikslais?“

Dėl proceso Teisingumo Teisme

80 2018 m. rugsėjo 25 d. Teisingumo Teismo pirmininko sprendimu bylos C-511/18 ir C-512/18 buvo sujungtos, kad būtų bendrai vykdoma rašytinė ir žodinė proceso dalys ir priimtas galutinis sprendimas. 2020 m. liepos 9 d. Teisingumo Teismo pirmininko sprendimu byla C-520/18 buvo sujungta su šiomis bylomis, kad būtų priimtas galutinis sprendimas.

Dėl prejudicinių klausimų

Dėl pirmųjų klausimų bylose C-511/18 ir C-512/18 ir dėl pirmojo ir antrojo klausimų byloje C-520/18

81 Pirmaisiais klausimais bylose C-511/18 ir C-512/18 ir pirmuoju ir antruoju klausimais byloje C-520/18, kuriuos reikia nagrinėti kartu, prašymus priimti prejudicinį sprendimą pateikę teismai iš esmės siekia išsiaiškinti, ar Direktyvos 2002/58 15 straipsnio 1 dalis turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, kuriais elektroninių ryšių paslaugų teikėjams nustatyta pareiga bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis šio 15 straipsnio 1 dalyje numatytais tikslais.

Pirminės pastabos

82 Iš Teisingumo Teismo turimos bylos medžiagos matyti, kad pagrindinėse bylose nagrinėjamos teisės nuostatos apima visas elektroninių ryšių priemones ir visus šių priemonių naudotojus, jų nediferencijuojant ir netaikant išimties. Be to, duomenys, kuriuos, remiantis šiais teisės aktais, turi saugoti elektroninių ryšių paslaugų teikėjai, visų pirma yra duomenys, būtini ryšio šaltiniui ir paskirčiai surasti, ryšio datai, valandai, trukmei ir tipui nustatyti, naudojami ryšio įrangai identifikuoti, taip pat galinei įrangos ir komunikacijos vietai nustatyti; tarp šių duomenų, be kita ko, yra naudotojo pavadinimas ir adresas, skambinančiojo ir adresato telefono numeriai bei IP adresas interneto paslaugoms. Vis dėlto minėti duomenys neapima atitinkamų pranešimų turinio.

83 Taigi duomenys, kurie pagal pagrindinėje byloje nagrinėjamus nacionalinės teisės aktus turi būti saugomi vienus metus, leidžia, be kita ko, nustatyti asmenį, su kuriuo elektroninio ryšio priemonės naudotojas komunikavo ir kokiomis priemonėmis tai buvo padaryta, taip pat komunikacijos ir interneto ryšių datą, laiką ir trukmę, vietą, iš kurios jie vyko, ir vietą, kur buvo galiniai įrenginiai, nors

pranešimas nebūtinai buvo perduotas. Be to, jie suteikia galimybę nustatyti, kaip dažnai vyko naudotojo ir tam tikrų asmenų komunikacija tam tikru laikotarpiu. Galiausiai, kalbant apie bylose C-511/18 ir C-512/18 nagrinėjamus nacionalinės teisės aktus, atrodo, kad jie, kiek apima ir duomenis, susijusius su elektroninių ryšių perdavimu tinklais, taip pat leidžia nustatyti internete naršomos informacijos pobūdį.

84 Dėl siekiamų tikslų reikia pažymėti, kad bylose C-511/18 ir C-512/18 nagrinėjamuose teisės aktuose, be kitų, numatyti šie tikslai: tirti, nustatyti baudžiamąsias veikas apskritai ir patraukti baudžiamojon atsakomybėn už jas, nacionalinis nepriklausomumas, teritorijos vientisumas ir nacionalinė gynyba, svarbūs užsienio politikos interesai, Prancūzijos europinių ir tarptautinių įsipareigojimų vykdymas, svarbiausi Prancūzijos ekonomikos, pramonės ir mokslo interesai, terorizmo, pasikėsinimų į respublikinę institucijų formą ir kolektyvinio smurto, galinčio rimtai pakenkti viešajai tvarkai, prevencija. Byloje C-520/18 nagrinėjamų teisės aktų tikslai, be kita ko, yra nusikalstamų veikų tyrimas, atskleidimas ir baudžiamasis persekiojimas, taip pat nacionalinio saugumo, teritorijos apsaugos ir visuomenės saugumo užtikrinimas.

85 Prašymus priimti prejudicinį sprendimą pateikę teismai visų pirma kelia klausimą dėl Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo galimo poveikio Chartijos 6 straipsnyje įtvirtintai teisei į saugumą. Be to, jiems kyla klausimas, ar Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymas, kurį lemia pagrindinėje byloje nagrinėjamuose teisės aktuose numatytas duomenų saugojimas, atsižvelgiant į tai, kad egzistuoja nacionalinių institucijų prieigą prie saugomų duomenų ribojančios taisyklės, gali būti laikomas pateisinamu. Be to, *Conseil d'État* (Valstybės Taryba) teigimu, kadangi šis klausimas kyla esant kontekstui, susijusiam su didele ir nuolatine grėsme nacionaliniam saugumui, jis taip pat turi būti vertinamas atsižvelgiant į ESS 4 straipsnio 2 dalį. *Cour constitutionnelle* (Konstitucinis Teismas) savo ruožtu pažymi, kad byloje C-520/18 nagrinėjamais nacionalinės teisės aktais taip pat įgyvendinami įpareigojimai veikti, kylantys iš Chartijos 4 ir 7 straipsnių, t. y. numatyti teisinį pagrindą, leidžiantį veiksmingai bausti už seksualinį nepilnamečių išnaudojimą.

86 Nors ir *Conseil d'État* (Valstybės Taryba), ir *Cour constitutionnelle* (Konstitucinis Teismas) remiasi prielaida, kad pagrindinėje byloje nagrinėjami nacionalinės teisės aktai, reglamentuojantys srauto ir vietos nustatymo duomenų saugojimą bei nacionalinių valdžios institucijų prieigą prie šių duomenų Direktyvos 2002/58 15 straipsnio 1 dalyje numatytais tikslais, pavyzdžiui, siekiant užtikrinti nacionalinį saugumą, patenka į šios direktyvos taikymo sritį, kai kurios pagrindinių bylų šalys ir kai kurios valstybės narės, pateikusios Teisingumo Teismui rašytines pastabas, šiuo klausimu turi skirtingą nuomonę, ypač kiek tai susiję su minėtos direktyvos 1 straipsnio 3 dalies aiškinimu. Taigi pirmiausia reikia išnagrinėti, ar minėti teisės aktai patenka į šios direktyvos taikymo sritį.

Direktyvos 2002/58 taikymo sritis

87 *Quadrature du Net*, *Fédération des fournisseurs d'accès à Internet associatifs*, *Igwan.net*, *Privacy International* ir *Center for Democracy and Technology*, remdamosi Teisingumo Teismo jurisprudencija dėl Direktyvos 2002/58 taikymo srities, iš esmės teigia, kad tiek duomenų saugojimas, tiek prieiga prie saugomų duomenų patenka į jos taikymo sritį, neatsižvelgiant į tai, ar prieiga suteikiama realiuoju laiku, ar ne. Iš tiesų, kadangi nacionalinio saugumo apsaugos tikslas aiškiai nurodytas šios direktyvos 15 straipsnio 1 dalyje, šio tikslo siekimas nereiškia, kad direktyva netaikoma. Prašymą priimti prejudicinį sprendimą pateikusių teismų nurodyta ESS 4 straipsnio 2 dalis neturi įtakos tokiam vertinimui.

88 Dėl žvalgybos priemonių, kurias kompetentingos Prancūzijos valdžios institucijos, nereguliuodamos elektroninių ryšių paslaugų teikėjų veiklos, tiesiogiai įgyvendina, nustatydamos tokiems teikėjams konkrečias pareigas, *Center for Democracy and Technology* pažymi, kad šios priemonės neišvengiamai patenka į Direktyvos 2002/58 ir Chartijos taikymo sritį, nes jos yra šios direktyvos 5 straipsnyje įtvirtinto konfidencialumo principo išimtys. Taigi minėtos priemonės turi atitikti iš direktyvos 15 straipsnio 1 dalies kylančius reikalavimus.

89 Vis dėlto Prancūzijos, Čekijos, Estijos vyriausybės, Airija, Kipro, Vengrijos, Lenkijos Švedijos ir Jungtinės Karalystės vyriausybės iš esmės teigia, kad Direktyva 2002/58 netaikoma nacionalinės teisės aktams, kaip antai nagrinėjamiems pagrindinėse bylose, nes jais siekiama užtikrinti nacionalinį saugumą. Žvalgybos tarnybų veikla, kiek ji susijusi su viešosios tvarkos palaikymu, vidaus saugumo ir teritorinio vientisumo užtikrinimu, priskirtina esminėms valstybių narių funkcijoms, todėl priklauso tik valstybių narių kompetencijai, kaip tai matyti, be kita ko, iš ESS 4 straipsnio 2 dalies trečio sakinio.

90 Šios vyriausybės ir Airija taip pat remiasi Direktyvos 2002/58 1 straipsnio 3 dalimi, pagal kurią į jos taikymo sritį nepatenka veikla, susijusi su visuomenės saugumu, gynyba ir valstybės saugumu, kaip tai jau buvo numatyta Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje. Šiuo klausimu jos remiasi 2006 m. gegužės 30 d. Sprendime *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346) pateiktu pastarosios nuostatos aiškinimu.

91 Reikia pažymėti, kad Direktyvos 2002/58 1 straipsnio 1 dalyje nurodyta, kad šioje direktyvoje, be kita ko, numatytas valstybių narių nuostatų, užtikrinančių vienodo lygio pagrindinių teisių ir laisvių, ypač teisės į privatų gyvenimą ir konfidencialumą, apsaugą, kiek tai susiję su asmens duomenų tvarkymu elektroninių ryšių sektoriuje, suderinimas.

92 Šios direktyvos 1 straipsnio 3 dalyje numatyta, kad ji netaikoma „valstybės veiksmams“ joje nurodytose srityse, įskaitant valstybės veiksmus baudžiamosios teisės srityje ir veiksmus, susijusius su visuomenės saugumu, gynyba, valstybės saugumu, taip pat valstybės ekonominę gerove, kai atitinkami veiksmai susiję su valstybės saugumo klausimais. Kaip pavyzdžiai nurodyta veikla visais atvejais yra pačių valstybių ar valstybės valdžios institucijų veikla, kuri nėra privačių asmenų veikla (2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 32 punktas ir jame nurodyta jurisprudencija).

93 Be to, Direktyvos 2002/58 3 straipsnyje numatyta, kad ši direktyva taikoma asmens duomenų tvarkymui, susijusiam su visuomenei prieinamų elektroninių ryšių paslaugų teikimu viešaisiais ryšių tinklais Sąjungoje, įskaitant viešuosius ryšių tinklus, palaikančius duomenų rinkimo ir atpažinimo įrenginius (toliau – elektroninių ryšių paslaugos). Taigi, reikia manyti, kad ši direktyva reglamentuoja tokių paslaugų teikėjų veiklą (2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 33 punktas ir jame nurodyta jurisprudencija).

94 Esant šioms aplinkybėms, pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybėms narėms leidžiama, laikantis joje nustatytų sąlygų, patvirtinti „[teisėkūros] priemones, ribojančias šios direktyvos 5 ir 6 straipsniuose, 8 straipsnio 1, 2, 3 ir 4 dalyse ir 9 straipsnyje nustatytų teisių ir pareigų taikymą“ (2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 71 punktas).

95 Direktyvos 2002/58 15 straipsnio 1 dalis neišvengiamai paremta prielaida, kad joje numatytos nacionalinės teisėkūros priemonės patenka į jos taikymo sritį, nes joje aiškiai nustatyta, kad valstybės narės gali jas patvirtinti, tik jeigu laikosi joje numatytų sąlygų. Be to, tokiomis priemonėmis šioje nuostatoje nurodytais tikslais reglamentuojama elektroninių ryšių paslaugų teikėjų veikla (2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 34 punktas ir jame nurodyta jurisprudencija).

96 Būtent atsižvelgdamas į šiuos argumentus Teisingumo Teismas nusprendė, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su jos 3 straipsniu, turi būti aiškinama taip, kad į šios direktyvos taikymo sritį patenka ne tik teisėkūros priemonė, kuria elektroninių ryšių paslaugų teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis, bet ir teisėkūros priemonė, pagal kurią jie įpareigojami kompetentingoms nacionalinėms institucijoms suteikti prieigą prie šių duomenų. Iš tiesų tokios teisėkūros priemonės neišvengiamai reiškia, kad minėti paslaugų teikėjai tvarko minėtus duomenis, ir jų negalima, kiek jomis reglamentuojama tų pačių teikėjų veikla, prilyginti pačių valstybių veiklai, numatytai minėtos direktyvos 1 straipsnio 3 dalyje (šiuo klausimu žr. 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 35 ir 37 punktus ir juose nurodytą jurisprudenciją).

97 Be to, atsižvelgiant į tai, kas išdėstyta šio sprendimo 95 punkte, ir į Direktyvos 2002/58 bendrą struktūrą, šios direktyvos aiškinimas, pagal kurį jos 15 straipsnio 1 dalyje nurodytos teisėkūros priemonės nepatenka į šios direktyvos taikymo sritį, nes tikslai, kuriems turi būti taikomos tokios priemonės, iš esmės sutampa su tikslais, kurių siekiama tos pačios direktyvos 1 straipsnio 3 dalyje nurodyta veikla, panaikintų bet kokį šios direktyvos 15 straipsnio 1 dalies veiksmingumą (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 72 ir 73 punktus).

98 Taigi Direktyvos 2002/58 1 straipsnio 3 dalyje vartojama sąvoka „veiklos rūšys“, kaip iš esmės pažymėjo generalinis advokatas savo išvados sujungtose bylose *La Quadrature du Net ir kt.* (C-511/18 ir C-512/18, EU:C:2020:6) 75 punkte, neturi būti aiškinama kaip apimanti šios direktyvos 15 straipsnio 1 dalyje nurodytas teisėkūros priemones.

99 Šios išvados negali paneigti ESS 4 straipsnio 2 dalies nuostatos, kuriomis remiasi šio sprendimo 89 punkte minėtos vyriausybės. Remiantis Teisingumo Teismo suformuota jurisprudencija, nors valstybės narės turi nustatyti savo esminius saugumo interesus ir imtis priemonių vidaus ir išorės saugumui užtikrinti, tik ta aplinkybė, kad buvo imtasi nacionalinės priemonės, siekiant užtikrinti nacionalinį saugumą, nereiškia, jog Sąjungos teisė netaikoma ir kad valstybės narės neturi jos laikytis, kaip reikalaujama (šiuo klausimu žr. 2013 m. birželio 4 d. Sprendimo *ZZ*, C-300/11, EU:C:2013:363, 38 punktą ir jame nurodytą jurisprudenciją; 2018 m. kovo 20 d. Sprendimo *Komisija / Austrija (Valstybinė spaustuvė)*, C-187/16, EU:C:2018:194, 75 ir 76 punktus; taip pat 2020 m. balandžio 2 d. Sprendimo *Komisija / Lenkija, Vengrija ir Čekijos Respublika (Laikinas tarptautinės apsaugos prašytojų perkėlimo mechanizmas)*, C-715/17, C-718/17 ir C-719/17, EU:C:2020:257, 143 ir 170 punktus).

100 Tiesa, kad 2006 m. gegužės 30 d. Sprendime *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346, 56–59 punktai) Teisingumo Teismas nusprendė, kad oro transporto bendrovių atliekamas asmens duomenų perdavimas trečiosios valstybės valdžios institucijoms, siekiant užkirsti kelią terorizmui ir kitoms sunkioms nusikalstamoms veikoms, remiantis Direktyvos 95/46 3 straipsnio 2 dalies pirma įtrauka, nepatenka į šios direktyvos taikymo sritį, nes šis perdavimas patenka į viešosios valdžios institucijų nustatytą sritį, susijusią su visuomenės saugumu.

101 Vis dėlto atsižvelgiant į šio sprendimo 93, 95 ir 96 punktuose nurodytus argumentus, šios jurisprudencijos negalima taikyti aiškinant Direktyvos 2002/58 1 straipsnio 3 dalį. Kaip iš esmės savo išvados sujungtose bylose *La Quadrature du Net ir kt.* (C-511/18 ir C-512/18, EU:C:2020:6) 70–72 punktuose nurodė generalinis advokatas, remiantis Direktyvos 95/46 3 straipsnio 2 dalies pirma įtrauka, su kuria susijusi minėta jurisprudencija, šios direktyvos taikymo sritis apskritai neapima „tvarkymo operacij[ų], susijusi[ų] su visuomenės saugumu, gynyba, valstybės saugumu“, neatsižvelgiant į tai, kas yra atitinkamų duomenų tvarkymo autorius. Tačiau aiškinant Direktyvos 2002/58 1 straipsnio 3 dalį atsižvelgti į tokį diferencijavimą būtina. Iš tiesų, kaip matyti iš šio sprendimo 94–97 punktų, bet koks elektroninių ryšių paslaugų teikėjų atliekamas asmens duomenų tvarkymas patenka į šios direktyvos taikymo sritį, įskaitant tvarkymą, kylantį iš valstybės valdžios institucijų jiems nustatytų įpareigojimų, nors prireikus tokiam tvarkymui gali būti taikoma Direktyvos 95/46 3 straipsnio 2 dalies pirmoje įtraukoje numatyta išimtis, atsižvelgiant į platesnę šios nuostatos formuluotę, apimančią bet kokį tvarkymą, nepriklausomai nuo autoriaus, kurio tikslas visuomenės saugumas, gynyba arba valstybės saugumas.

102 Be to, reikia pažymėti, kad Direktyva 95/46, nagrinėta byloje, kurioje priimtas 2006 m. gegužės 30 d. Sprendimas *Parlamentas / Taryba ir Komisija* (C-317/04 ir C-318/04, EU:C:2006:346), pagal Reglamento 2016/679 94 straipsnio 1 dalį nuo 2018 m. gegužės 25 d. buvo panaikinta ir pakeista šiuo reglamentu. Nors minėto reglamento 2 straipsnio 2 dalies d punkte nurodyta, kad jis netaikomas, kai duomenis tvarko „kompetentingos valdžios institucijos“, siekdamos užkirsti kelią nusikalstamoms veikoms ir jas nustatyti, įskaitant apsaugą nuo grėsmės visuomenės saugumui ir tokios grėsmės prevenciją, iš to paties reglamento 23 straipsnio 1 dalies d ir h punktų matyti, kad asmens duomenų tvarkymas, kurį tuo pačiu tikslu atlieka privatūs asmenys, patenka į šio reglamento taikymo sritį.

Darytina išvada, kad prieš tai pateiktas Direktyvos 2002/58 1 straipsnio 3 dalies, 3 straipsnio ir 15 straipsnio 1 dalies aiškinimas atitinka Reglamento 2016/679 taikymo srities apibrėžimą, kurį papildo ir patikslina ši direktyva.

103 Vis dėlto, kai valstybės narės tiesiogiai įgyvendina priemones, nukrypstančias nuo elektroninių ryšių konfidencialumo, nenustatydamos tokių ryšių paslaugų teikėjams pareigos tvarkyti duomenis, duomenų subjektų duomenų apsaugai taikoma ne Direktyva 2002/58, o tik nacionalinė teisė, išskyrus atvejus, kai taikoma 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuria panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (OL L 119, 2016, p. 89; klaidų ištaisymas OL L 127, 2018, p. 6), todėl nagrinėjamos priemonės turi visų pirma atitikti konstitucinio lygio nacionalinę teisę ir EŽTK reikalavimus.

104 Iš to, kas išdėstyta, matyti, kad nacionalinės teisės aktai, kaip antai nagrinėjami pagrindinėse bylose, kuriais elektroninių ryšių paslaugų teikėjai įpareigojami saugoti srauto ir vietos nustatymo duomenis, siekiant apsaugoti nacionalinį saugumą ir kovoti su nusikalstamumu, patenka į Direktyvos 2002/58 taikymo sritį.

Dėl Direktyvos 2002/58 15 straipsnio 1 dalies aiškinimo

105 Pirmiausia reikia priminti, kad pagal suformuotą jurisprudenciją aiškinant Sąjungos teisės nuostatą reikia remtis ne tik jos tekstu, bet ir jos kontekstu bei teisės akto, kuriame ji įtvirtinta, tikslais, taip pat, be kita ko, atsižvelgti į šių teisės aktų genezę (šiuo klausimu žr. 2018 m. balandžio 17 d. Sprendimo *Egenberger*, C-414/16, EU:C:2018:257, 44 punktą).

106 Direktyva 2002/58, kaip matyti, be kita ko, iš jos 6 ir 7 konstatuojamųjų dalių, siekiama apsaugoti elektroninių ryšių paslaugų naudotojus nuo pavojaus, kuris asmens duomenims ir privačiam gyvenimui kyla dėl naujųjų technologijų ir ypač dėl didėjančių automatizuoto duomenų kaupimo ir tvarkymo pajėgumų. Visų pirma minėta direktyva, kaip nurodyta jos 2 konstatuojamojoje dalyje, siekiama užtikrinti visapusišką Chartijos 7 ir 8 straipsniuose išdėstytų teisių paisymą. Šiuo klausimu pažymėtina, kad iš Europos Parlamento ir Tarybos direktyvos dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje pasiūlymo (COM(2000) 385 *final*), kuriuo remiantis parengta Direktyva 2002/58, aiškinamojo memorandumo matyti, jog Sąjungos teisės aktų leidėjas siekė „užtikrinti, kad ir toliau būtų laikomasi asmens duomenų ir privataus gyvenimo aukšto lygio apsaugos visų elektroninių ryšių paslaugų atveju, nepaisant naudojamos technologijos“.

107 Šiuo tikslu Direktyvos 2002/58 5 straipsnio 1 dalyje įtvirtintas elektroninių pranešimų ir su jais susijusių srauto duomenų konfidencialumo principas, kuris, be kita ko, reiškia, kad iš esmės bet kuriam asmeniui, išskyrus naudotoją, draudžiama saugoti šiuos pranešimus ir duomenis be jo sutikimo.

108 Konkrečiai kalbant apie elektroninių ryšių paslaugų teikėjų atliekamą srauto duomenų tvarkymą ir saugojimą, iš Direktyvos 2002/58 6 straipsnio ir 22 bei 26 konstatuojamųjų dalių matyti, kad leidžiamas tokios apimties ir tiek laiko trunkantis tvarkymas, kiek būtina tokių paslaugų rinkodarai, sąskaitoms už jas išrašyti ir teikti pridėtinės vertės paslaugoms. Pasibaigus šiam terminui, tvarkomi ir saugomi duomenys turi būti sunaikinti arba anoniminti. Kiek tai susiję su vietos nustatymo duomenimis, kurie nėra srauto duomenys, minėtos direktyvos 9 straipsnio 1 dalyje numatyta, kad tokie duomenys gali būti tvarkomi tik kai tenkinamos tam tikros sąlygos ir kai jie buvo anoniminti, arba kai tam gautas naudotojų ar abonentų sutikimas (2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 86 punktas ir jame nurodyta jurisprudencija).

109 Taigi priimdamas šią direktyvą Sąjungos teisės aktų leidėjas sukonkretino Chartijos 7 ir 8 straipsniuose įtvirtintas teises taip, kad elektroninių ryšių priemonių naudotojai iš esmės turi teisę tikėtis, jog be jų sutikimo jų pranešimai ir su jais susiję duomenys išliks anonimiški ir negalės būti registruojami.

110 Vis dėlto pagal Direktyvos 2002/58 15 straipsnio 1 dalį valstybėms narėms leidžiama nustatyti šios direktyvos 5 straipsnio 1 dalyje įtvirtintos pagrindinės pareigos užtikrinti asmens duomenų konfidencialumą ir susijusių pareigų, nurodytų, be kita ko, šios direktyvos 6 ir 9 straipsniuose, išimtis, jeigu toks ribojimas yra demokratinėje visuomenėje būtina, tinkama ir proporcinga priemonė, skirta apsaugoti nacionaliniam ir visuomenės saugumui, gynybai arba užtikrinti nusikalstamų veikų ar neteisėto elektroninių ryšių sistemos naudojimo prevencijai, tyrimui, atskleidimui ar baudžiamajam persekiojimui už jas. Šiuo tikslu valstybės narės gali, *inter alia*, patvirtinti teisėkūros priemones, leidžiančias ribotą laikotarpį saugoti duomenis, kai tai pateisinama viena iš nurodytų priežasčių.

111 Atsižvelgiant į tai, galimybė nukrypti nuo Direktyvos 2002/58 5, 6 ir 9 straipsniuose numatytų teisių ir pareigų negali pateisinti to, kad pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą ir ypač šios direktyvos 5 straipsnyje aiškiai numatyto draudimo saugoti šiuos duomenis išimtis taptų taisykle (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 89 ir 104 punktus).

112 Dėl tikslų, galinčių pateisinti teisių ir pareigų, numatytų, be kita ko, Direktyvos 2002/58 5, 6 ir 9 straipsniuose, apribojimą, Teisingumo Teismas jau yra nusprendęs, kad šios direktyvos 15 straipsnio 1 dalies pirmame sakinyje pateiktas tikslų sąrašas yra baigtinis, todėl pagal šią nuostatą priimta teisėkūros priemonė turi iš tikrųjų griežtai atitikti vieną iš šių tikslų (šiuo klausimu žr. 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 52 punktą ir jame nurodytą jurisprudenciją).

113 Be to, iš Direktyvos 2002/58 15 straipsnio 1 dalies trečio sakinio matyti, kad valstybėms narėms leidžiama imtis teisėkūros priemonių, kuriomis siekiama apriboti šios direktyvos 5, 6 ir 9 straipsniuose nurodytų teisių ir pareigų apimtį, tik laikantis bendrųjų Sąjungos teisės principų, įskaitant proporcingumo principą, ir Chartijoje garantuojamų pagrindinių teisių. Šiuo klausimu Teisingumo Teismas jau yra nusprendęs, kad elektroninių ryšių paslaugų teikėjams valstybės narės nacionalinės teisės aktuose nustatyta pareiga saugoti srauto duomenis, kad prireikus jie būtų prieinami kompetentingoms nacionalinėms institucijoms, kelia klausimų ne tik dėl Chartijos 7 ir 8 straipsnių, susijusių atitinkamai su privataus gyvenimo ir asmens duomenų apsaugos užtikrinimu, bet ir dėl Chartijos 11 straipsnyje garantuojamos saviraiškos laisvės paisymo (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 25 ir 70 punktus; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 91 ir 92 punktus bei juose nurodytą jurisprudenciją).

114 Taigi aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį reikia atsižvelgti tiek į Chartijos 7 straipsnyje įtvirtintą teisę į privataus gyvenimą gerbimą, tiek į jos 8 straipsnyje įtvirtintos teisės į asmens duomenų apsaugą svarbą, kaip matyti iš Teisingumo Teismo jurisprudencijos, taip pat į saviraiškos laisvę, t. y. Chartijos 11 straipsnyje garantuojamą pagrindinę teisę – vieną iš pagrindinių demokratinės ir pliuralistinės visuomenės pagrindų, kurie yra vertybių, kuriomis pagal ESS 2 straipsnį grindžiama Sąjunga, dalis (šiuo klausimu žr. 2001 m. kovo 6 d. Sprendimo *Connolly / Komisija*, C-274/99 P, EU:C:2001:127, 39 punktą; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 93 punktą ir jame nurodytą jurisprudenciją).

115 Šiuo klausimu reikia patikslinti, kad srauto ir vietos nustatymo duomenų saugojimas savaime yra, pirma, Direktyvos 2002/58 5 straipsnio 1 dalyje numatyto draudimo saugoti šiuos duomenis, taikomo bet kuriam asmeniui, kuris nėra naudotojas, išimtis ir, antra, Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių į privataus gyvenimo gerbimą ir asmens duomenų apsaugą suvaržymas, neatsižvelgiant į tai, ar atitinkama informacija, susijusi su privačiu gyvenimu, yra jautri, ar ne, ir ar suinteresuotieji asmenys patyrė nepatogumų dėl tokio suvaržymo (šiuo klausimu žr. 2017 m. liepos

26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 124 ir 126 punktus ir juose nurodytą jurisprudenciją; pagal analogiją, kiek tai susiję su EŽTK 8 straipsniu, žr. 2020 m. sausio 30 d. EŽTT sprendimo *Breyer prieš Vokietiją*, CE:ECHR:2020:0130JUD005000112, 81 punktą).

116 Taip pat, nepaisant to, ar saugomi duomenys vėliau naudojami, ar ne (pagal analogiją, kiek tai susiję su EŽTK 8 straipsniu, žr. 2000 m. vasario 16 d. EŽTT sprendimo *Amann prieš Šveicariją*, CE:ECHR:2000:0216JUD002779895, 69 punktą; taip pat 2020 m. vasario 13 d. Sprendimo *Trjakovski ir Chipovski prieš Šiaurės Makedoniją*, CE:ECHR:2020:0213JUD005320513, 51 punktą), prieiga prie tokių duomenų, nepriklausomai nuo jų vėlesnio naudojimo, yra atskiras pagrindinių teisių, nurodytų pirmesniame šio sprendimo punkte, suvaržymas (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 124 ir 126 punktus).

117 Ši išvada yra juo labiau pagrįsta dėl to, kad srauto ir vietos nustatymo duomenys gali atskleisti daug svarbių aspektų apie duomenų subjektų privatų gyvenimą, įskaitant jautrią informaciją, pavyzdžiui, seksualinę orientaciją, politines pažiūras, religinius, filosofinius, socialinius ar kitus įsitikinimus ir sveikatos būklę, nors šiems duomenims, be kita ko, Sąjungos teisėje taikoma ypatinga apsauga. Iš šių duomenų, vertinamų kaip visuma, gali būti daromos labai tikslios išvados apie asmenų, kurių duomenys saugomi, privatų gyvenimą, kaip antai kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ir kitokį judėjimą, vykdomą veiklą, socialinius ryšius ir jų socialinę aplinką. Visų pirma šie duomenys sudaro sąlygas duomenų subjektų profiliui nustatyti, o tai irgi yra tokia pat jautri informacija, kiek tai susiję su teise į privataus gyvenimo gerbimą, kaip ir pranešimų turinys (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 27 punktą; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 99 punktą).

118 Taigi, pirma, srauto ir vietos nustatymo duomenų saugojimu teisėsaugos tikslais gali būti savaime pažeista Chartijos 7 straipsnyje įtvirtinta teisė į komunikacijos slaptumą ir tai gali turėti atgrasomąjį poveikį elektroninių ryšių priemonių naudotojams įgyvendinti Chartijos 11 straipsnyje garantuojamą jų saviraiškos laisvę (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 28 punktą; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 101 punktą). Toks atgrasomasis poveikis gali daryti poveikį visų pirma asmenims, kurių komunikacijai pagal nacionalines taisykles taikoma profesinės paslapties apsauga, ir pranešėjams, kurių veikla saugoma pagal 2019 m. spalio 23 d. Europos Parlamento ir Tarybos direktyvą (ES) 2019/1937 dėl asmenų, pranešančių apie Sąjungos teisės pažeidimus, apsaugos (OL L 305, 2019, p. 17). Be to, šis poveikis yra tuo didesnis, kuo didesnė duomenų apimtis ir jų įvairovė.

119 Antra, atsižvelgiant į didelį srauto ir vietos nustatymo duomenų, kurie gali būti nuolat saugomi taikant bendrą ir nediferencijuotą saugojimo priemonę, kiekį ir į informacijos, kurią šie duomenys gali suteikti, jautrumą, vien elektroninių ryšių paslaugų teikėjų atliekamas šių duomenų saugojimas kelia piktnaudžiavimo ir neteisėtos prieigos pavojų.

120 Taigi tiek, kiek ja valstybėms narėms leidžiama nustatyti šio sprendimo 110 punkte numatytas išimtis, Direktyvos 2002/58 15 straipsnio 1 dalis atspindi tai, kad Chartijos 7 ir 8 straipsniuose įtvirtintos teisės nėra absoliučios ir turi būti vertinamos atsižvelgiant į jų visuomeninę paskirtį (šiuo klausimu žr. 2020 m. liepos 16 d. Sprendimo *Facebook Ireland ir Schrems*, C-311/18, EU:C:2020:559, 172 punktą ir jame nurodytą jurisprudenciją).

121 Iš tiesų, kaip matyti iš Chartijos 52 straipsnio 1 dalies, ja leidžiama apriboti naudojimąsi tokiomis teisėmis, jei šie apribojimai numatyti įstatymo, nekeičia minėtų teisių esmės ir, remiantis proporcingumo principu, yra būtini ir tikrai atitinka Sąjungos pripažintus bendruosius interesus arba reikalingi kitų teisėms ir laisvėms apsaugoti.

122 Taigi, aiškinant Direktyvos 2002/58 15 straipsnio 1 dalį atsižvelgiant į Chartiją, taip pat reikia atsižvelgti į Chartijos 3, 4, 6 ir 7 straipsniuose įtvirtintų teisių ir nacionalinio saugumo bei kovos su sunkiais nusikaltimais tikslų svarbą, prisidedant prie kitų asmenų teisių ir laisvių apsaugos.

123 Šiuo klausimu pažymėtina, kad Chartijos 6 straipsnyje, kuriuo remiasi *Conseil d'État* (Valstybės Taryba) ir *Cour constitutionnelle* (Konstitucinis Teismas) įtvirtinta kiekvieno asmens teisė ne tik į laisvę, bet ir į saugumą ir užtikrinamos teisės, atitinkančios EŽTK 5 straipsnyje įtvirtintas teises (šiuo klausimu žr. 2016 m. vasario 15 d. Sprendimo *N.*, C-601/15 PPU, EU:C:2016:84, 47 punktą; 2016 m. liepos 28 d. Sprendimo *JZ*, C-294/16 PPU, EU:C:2016:610, 48 punktą ir 2019 m. rugsėjo 19 d. Sprendimo *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, 42 punktą ir jame nurodytą jurisprudenciją).

124 Be to, reikia priminti, kad Chartijos 52 straipsnio 3 dalimi siekiama užtikrinti būtiną Chartijoje įtvirtintų teisių ir atitinkamų EŽTK garantuojamų teisių darną, nepažeidžiant Sąjungos teisės ir Europos Sąjungos Teisingumo Teismo autonomijos. Taigi, siekiant aiškinti Chartiją, reikia atsižvelgti į atitinkamas EŽTK garantuojamas teises kaip į minimalų apsaugos lygį (šiuo klausimu žr. 2019 m. vasario 12 d. Sprendimo *TC*, C-492/18 PPU, EU:C:2019:108, 57 punktą ir 2019 m. gegužės 21 d. Sprendimo *Komisija / Vengrija (Žemės ūkio paskirties žemės uzufruktas)*, C-235/17, EU:C:2019:432, 72 punktą ir jame nurodytą jurisprudenciją).

125 EŽTK 5 straipsniu, kuriame įtvirtinta „teisė į laisvę“ ir „teisė į saugumą“, remiantis Europos Žmogaus Teisių Teismo jurisprudencija, siekiama apsaugoti asmenį nuo bet kokio savavališko ar nepateisinamo laisvės atėmimo (šiuo klausimu žr. 2008 m. kovo 18 d. EŽTT sprendimo *Ladent prieš Lenkiją*, CE:ECHR:2008:0318JUD001103603, 45 ir 46 punktus; 2010 m. kovo 29 d. EŽTT sprendimo *Medvedyev ir kiti prieš Prancūziją*, CE:ECHR:2010:0329JUD000339403, 76 ir 77 punktus ir 2012 m. gruodžio 13 d. EŽTT sprendimo *El-Masri prieš „The former Yugoslav Republic of Macedonia“*, CE:ECHR:2012:1213JUD003963009, 239 punktą). Vis dėlto, kadangi ši nuostata susijusi su viešosios valdžios institucijos nustatytu laisvės atėmimu, Chartijos 6 straipsnio negalima aiškinti taip, kad juo viešosios valdžios institucijoms nustatoma pareiga imtis konkrečių priemonių, kad būtų užkirstas kelias tam tikroms nusikalstamoms veikoms.

126 Priešingai, kiek tai susiję su *Cour constitutionnelle* (Konstitucinis Teismas) nurodyta kova su nusikalstamomis veikomis, kurių aukos yra visų pirma nepilnamečiai ir kiti pažeidžiami asmenys, reikia pabrėžti, kad pareigos veikti, tenkančios viešosios valdžios institucijoms, gali kilti iš Chartijos 7 straipsnio, siekiant priimti teisines priemones, kuriomis siekiama apsaugoti privatų ir šeimos gyvenimą (šiuo klausimu žr. 2020 m. birželio 18 d. Sprendimo *Komisija / Vengrija (Asociacijų skaidrumas)*, C-78/18, EU:C:2020:476, 123 punktą ir jame nurodytą Europos Žmogaus Teisių Teismo jurisprudenciją). Tokios pareigos taip pat gali išplaukti iš minėto 7 straipsnio, kiek tai susiję su būsto neliečiamybe ir komunikacijos slaptumu, bei iš 3 ir 4 straipsnių, susijusių su asmenų fizine ir psichine neliečiamybe bei kankinimo, nežmoniško ir žeminamo elgesio draudimu.

127 Atsižvelgiant į šias įvairias pareigas veikti, reikia suderinti įvairius nagrinėjamus interesus ir teises.

128 Europos Žmogaus Teisių Teismas yra nusprendęs, kad pareigos veikti, kylančios iš EŽTK 3 ir 8 straipsnių, kurių atitinkamos garantijos įtvirtintos Chartijos 4 ir 7 straipsniuose, apima, be kita ko, materialinių ir procesinių nuostatų priėmimą ir praktines priemones, leidžiančias veiksmingai kovoti su nusikalstamomis veikomis prieš asmenis, atliekant tyrimą ir vykdant veiksmingą baudžiamąjį persekiojimą; ši pareiga yra dar svarbesnė, kai kyla grėsmė vaiko fizinei ir moralinei gerovei. Taigi priemonės, kurių turi imtis kompetentingos institucijos, turi visiškai atitikti teisines priemones ir kitas garantijas, kuriomis gali būti apribota įgaliojimų vykdyti baudžiamąjį persekiojimą apimtis bei kitos laisvės ir teisės. Konkrečiai kalbant, to teismo teigimu, reikia nustatyti teisinį pagrindą, kuris leistų suderinti skirtingus saugotinus interesus ir teises (1998 m. spalio 28 d. EŽTT sprendimo *Osman prieš Jungtinę Karalystę*, CE:ECHR:1998:1028JUD002345294, 115 ir 116 punktai; 2004 m. kovo 4 d. EŽTT sprendimo *M.C. prieš Bulgariją*, CE:ECHR:2003:1204JUD003927298, 151 punktas; 2004 m. birželio

24 d. EŽTT sprendimo *Von Hannover prieš Vokietiją*, CE:ECHR:2004:0624JUD005932000, 57 ir 58 punktai ir 2008 m. gruodžio 2 d. EŽTT sprendimo *K.U. prieš Suomiją*, CE:ECHR:2008:1202JUD 000287202, 46, 48 ir 49 punktai).

129 Dėl proporcingumo principo paisymo reikia pabrėžti, kad Direktyvos 2002/58 15 straipsnio 1 dalies pirmame sakinyje numatyta, kad valstybės narės gali nustatyti nuo pranešimų ir su jais susijusių srauto duomenų konfidencialumo pareigos nukrypstančią priemonę, kai ji yra „būtina, tinkama ir adekvati [proporcinga] demokratinė[je] visuomenė[je] priemonė“ atsižvelgiant į šia nuostata siekiamus tikslus. Minėtos direktyvos 11 konstatuojamojoje dalyje patikslinama, kad tokio pobūdžio priemonė turi „griežtai“ atitikti siekiamą tikslą.

130 Šiuo klausimu reikia priminti, kad pagrindinės teisės į privataus gyvenimo gerbimą apsauga reikalauja, remiantis suformuota Teisingumo Teismo jurisprudencija, kad nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neviršytų to, kas yra griežtai būtina. Be to, bendrojo intereso tikslo negalima siekti neatsižvelgiant į tai, kad jis turi būti derinamas su pagrindinėmis teisėmis, kurioms taikoma priemonė, nustatant pusiausvyrą tarp, viena vertus, bendrojo intereso tikslo ir, kita vertus, nagrinėjamų teisių (šiuo klausimu žr. 2008 m. gruodžio 16 d. Sprendimo *Satakunnan Markkinapörssi ir Satamedia*, C-73/07, EU:C:2008:727, 56 punktą; 2010 m. lapkričio 9 d. Sprendimo *Volker und Markus Schecke ir Eifert*, C-92/09 ir C-93/09, EU:C:2010:662, 76, 77 ir 86 punktus; 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 52 punktą ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 140 punktą).

131 Konkrečiau kalbant, iš Teisingumo Teismo jurisprudencijos matyti, kad valstybių narių galimybė pateisinti teisių ir pareigų, numatytų, be kita ko, Direktyvos 2002/58 5, 6 ir 9 straipsniuose, apribojimą turi būti vertinama atsižvelgiant į suvaržymo, kurį lemia toks apribojimas, dydį ir tikrinant, ar šiuo apribojimu siekiamo bendrojo intereso tikslo svarba jį atitinka (šiuo klausimu žr. 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 55 punktą ir jame nurodytą jurisprudenciją).

132 Tam, kad atitiktų proporcingumo reikalavimą, teisės aktuose turi būti numatytos aiškios ir tikslios taisyklės, reglamentuojančios nagrinėjamos priemonės apimtį ir taikymą bei nustatančios minimalius reikalavimus, kad asmenys, kurių asmens duomenys tvarkomi, turėtų pakankamai garantijų, leidžiančių veiksmingai apsaugoti šiuos duomenis nuo piktnaudžiavimo pavojų. Tokie teisės aktai turi būti teisiškai privalomi pagal nacionalinę teisę ir juose turi būti nurodyta, kokiomis aplinkybėmis ir sąlygomis gali būti imtasi tokios duomenų tvarkymą numatančios priemonės, taip užtikrinant, kad teisių suvaržymas neviršytų to, kas griežtai būtina. Būtinybė turėti tokias garantijas yra dar svarbesnė tais atvejais, kai asmens duomenys tvarkomi automatizuotai, visų pirma kai egzistuoja didelis neteisėtos prieigos prie šių duomenų pavojus. Šios išvados ypač taikytinos tais atvejais, kai susiduriama su šios ypatingos asmens duomenų kategorijos, kokią sudaro jautrūs duomenys, apsaugos klausimu (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 54 ir 55 punktus; 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 117 punktą ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 141 punktą).

133 Taigi teisės aktai, kuriuose numatytas asmens duomenų saugojimas, visada turi atitikti objektyvius kriterijus, nustatančius saugotinų asmens duomenų ir siekiamo tikslo ryšį (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 191 punktą ir jame nurodytą jurisprudenciją ir 2019 m. spalio 3 d. Sprendimo *A ir kt.*, C-70/18, EU:C:2019:823, 63 punktą).

– Dėl teisėkūros priemonių, kuriomis numatoma prevenciškai saugoti srauto ir vietos nustatymo duomenis, siekiant užtikrinti nacionalinį saugumą

134 Reikia pažymėti, kad Teisingumo Teismas savo sprendimuose, kuriuose aiškinama Direktyva 2002/58, dar nėra konkrečiai išnagrinėjęs nacionalinio saugumo užtikrinimo tikslo, kurį nurodo prašymą priimti prejudicinį sprendimą pateikę teismai ir pastabas pateikusios vyriausybės.

135 Šiuo klausimu pirmiausia reikia pažymėti, kad ESS 4 straipsnio 2 dalyje nustatyta, jog kiekviena valstybė narė išimtinai išlieka atsakinga už nacionalinį saugumą. Ši atsakomybė atitinka pagrindinį interesą apsaugoti esmines valstybės funkcijas ir pagrindinius visuomenės interesus ir apima veiklos, galinčios rimtai destabilizuoti pagrindines valstybės konstitucines, politines, ekonomines ar socialines struktūras ir visų pirma keliančios tiesioginį pavojų pačiai visuomenei, gyventojams ar valstybei, pavyzdžiui, teroristinės veiklos, prevenciją ir baudžiamąjį persekiojimą už ją.

136 Nacionalinio saugumo užtikrinimo tikslo, siejamo su ESS 4 straipsnio 2 dalimi, svarba viršija kitų Direktyvos 2002/58 15 straipsnio 1 dalyje nurodytų tikslų, be kita ko, kovos su nusikalstamumu apskritai, net ir su sunkiais nusikaltimais, ir visuomenės saugumo užtikrinimo tikslų svarbą. Iš tiesų pirmesniame punkte nurodytos grėsmės savo pobūdžiu ir ypatingu sunkumu skiriasi nuo bendros įtampos ar sutrikimų, net didelių, rizikos visuomenės saugumui. Taigi su sąlyga, kad bus laikomasi kitų Chartijos 52 straipsnio 1 dalyje numatytų reikalavimų, nacionalinio saugumo užtikrinimo tikslas gali pateisinti priemones, numatančias didesnį pagrindinių teisių suvaržymą nei tas, kurį būtų galima pateisinti kitais tikslais.

137 Taigi, esant tokioms situacijoms, kokios aprašytos šio sprendimo 135 ir 136 punktuose, pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, iš esmės nedraudžiama tokia teisėkūros priemonė, pagal kurią kompetentingoms institucijoms leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus saugoti srauto ir vietos nustatymo duomenis, susijusius su visais elektroninio ryšio priemonių naudotojais ribotą laikotarpį, jeigu yra pakankamai konkrečių aplinkybių, leidžiančių manyti, kad atitinkamos valstybės nacionaliniam saugumui kyla didelė grėsmė – tokia, kaip nurodyta šio sprendimo 135 ir 136 punktuose, kuri yra tikra, esama ar numatoma. Nors tokia priemonė nediferencijuotai taikoma visiems elektroninių ryšių priemonių naudotojams, kurie iš pirmo žvilgsnio neatrodo esantys susiję, kaip tai suprantama pagal šio sprendimo 133 punkte nurodytą jurisprudenciją, su grėsme šios valstybės narės nacionaliniam saugumui, vis dėlto reikia konstatuoti, kad tokios grėsmės buvimas savaime gali būti tokios sąsajos įrodymas.

138 Vis dėlto įpareigojimas prevenciškai saugoti visų elektroninių ryšių priemonių naudotojų duomenis turi būti apribotas laiko atžvilgiu tuo, kas griežtai būtina. Nors negalima atmesti galimybės, kad elektroninių ryšių paslaugų teikėjams nustatytas įpareigojimas saugoti duomenis gali būti pratęstas dėl to, kad išlieka tokia grėsmė, kiekvieno įpareigojimo trukmė negali būti ilgesnė nei tam tikras numatomas laikotarpis. Be to, tokiam duomenų saugojimui turi būti taikomi apribojimai ir nustatytos griežtos garantijos, leidžiančios veiksmingai apsaugoti duomenų subjektų asmens duomenis nuo piktnaudžiavimo pavojaus. Taigi toks saugojimas negali būti sisteminis.

139 Atsižvelgiant į Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymo, kurį lemia tokia bendro ir nediferencijuoto duomenų saugojimo priemonė, dydį, svarbu užtikrinti, kad šia priemone būtų veiksmingai naudojamasi tik tais atvejais, kai kyla didelė grėsmė nacionaliniam saugumui, kaip antai nurodytais šio sprendimo 135 ir 136 punktuose. Šiuo tikslu labai svarbu, kad sprendimui, kuriuo elektroninių ryšių paslaugų teikėjai įpareigojami saugoti duomenis, galėtų būti taikoma veiksminga teismo arba nepriklausomos administracinio subjekto, kurio sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi sąlygų ir garantijų, kurios turi būti numatytos.

– Dėl teisėkūros priemonių, kuriomis numatoma prevenciškai saugoti srauto ir vietos nustatymo duomenis, siekiant kovoti su nusikalstamumu ir užtikrinti visuomenės saugumą

140 Kiek tai susiję su nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo už jas tikslu, pagal proporcingumo principą tik kova su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencija gali pateisinti didelius Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymus, kaip antai susijusius su srauto ir vietos nustatymo duomenų saugojimu. Taigi nedideli minėtų teisių suvaržymai gali būti pateisinami tikslu užtikrinti nusikalstamų veikų prevenciją, tyrimą, nustatymą ir baudžiamąjį persekiojimą už jas apskritai (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 102 punktą; 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 56 ir 57 punktus ir 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 149 punktą).

141 Nacionalinės teisės aktai, kuriuose numatytas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas, siekiant kovoti su sunkiais nusikaltimais, viršija tai, kas griežtai būtina, ir negali būti laikomi pateisinamais demokratinėje visuomenėje, kaip to reikalaujama pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 107 punktą).

142 Iš tiesų atsižvelgiant į informacijos, kurią gali suteikti srauto ir vietos nustatymo duomenys, jautrumą, šios informacijos konfidencialumas yra esminis, kiek tai susiję su teise į privataus gyvenimo gerbimą. Taigi, atsižvelgiant į atgrasomąjį poveikį Chartijos 7 ir 11 straipsniuose įtvirtintoms pagrindinėms teisėms, nurodytoms šio sprendimo 118 punkte, kurį gali sukelti šių duomenų saugojimas, ir į suvaržymo, kurį lemia toks saugojimas, dydį, demokratinėje visuomenėje svarbu, kad, kaip numatyta Direktyva 2002/58 nustatytoje sistemoje, šis saugojimas būtų išimtis, o ne taisyklė ir kad šie duomenys nebūtų sistemingai ir nuolat saugomi. Ši išvada darytina net ir dėl kovos su sunkiais nusikaltimais ir didelės grėsmės visuomenės saugumui prevencijos tikslų bei atsižvelgiant į jiems teiktiną svarbą.

143 Be to, Teisingumo Teismas pabrėžė, kad teisės aktai, kuriuose numatytas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas, apima beveik visų gyventojų elektroninius pranešimus, nedarant jokio skirtumo, apribojimo ar išimties dėl siekiamo tikslo. Tokie teisės aktai, priešingai reikalavimui, primintam šio sprendimo 133 punkte, taikomi bendrai visiems asmenims, kurie naudojasi elektroninių ryšių paslaugomis, o šių asmenų padėtis, net netiesiogiai, nėra tokia, dėl kurios gali būti pradėtas baudžiamasis persekiojimas. Taigi jie taikomi net tiems asmenims, dėl kurių neegzistuoja jokių požymių, leidžiančių manyti, kad jų elgesys gali turėti bent netiesioginį ar tolimą ryšį su tikslu kovoti su sunkiais nusikaltimais, visų pirma nenustačius ryšio tarp duomenų, kuriuos numatyta saugoti, ir grėsmės visuomenės saugumui (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 57 ir 58 punktus; taip pat 2016 m. gruodžio 21 d. Sprendimo *Tele2* C-203/15 ir C-698/15, EU:C:2016:970, 105 punktą).

144 Visų pirma, kaip jau yra nusprendęs Teisingumo Teismas, tokiuose teisės aktuose nenustatyta, kad saugomi tik tie duomenys, kurie susiję su tam tikru laikotarpiu ir (arba) geografine zona, ir (arba) asmenų, kurie, vienaip ar kitaip, galėtų būti siejami su vienu iš sunkių nusikaltimų, ratu arba asmenimis, kurių duomenų saugojimas galėtų prisidėti prie kovos su sunkiomis nusikalstamomis veikomis (šiuo klausimu žr. 2014 m. balandžio 8 d. Sprendimo *Digital Rights*, C-293/12 ir C-594/12, EU:C:2014:238, 59 punktą ir 2016 m. gruodžio 21 d. Sprendimo *Tele2* C-203/15 ir C-698/15, EU:C:2016:970, 106 punktą).

145 Net valstybių narių pareigomis veikti, kurios tam tikrais atvejais gali kilti iš Chartijos 3, 4 ir 7 straipsnių ir kurios, kaip pažymėta šio sprendimo 126 ir 128 punktuose, susijusios su taisyklių, leidžiančių veiksmingai kovoti su nusikalstamomis veikomis, nustatymu, negalima pateisinti tokių didelių suvaržymų, kokie nustatyti teisės aktuose, numatančiuose srauto ir vietos nustatymo duomenų

saugojimą, kiek tai susiję su Chartijos 7 ir 8 straipsniuose įtvirtintomis pagrindinėmis beveik visų gyventojų teisėmis, kai negali būti nustatytas, bent jau netiesioginis, duomenų subjektų duomenų ir siekiamo tikslo ryšys.

146 Vis dėlto atsižvelgiant į tai, kas nurodyta šio sprendimo 142–144 punktuose, ir į būtiną nagrinėjamų teisių ir interesų suderinimą, kovos su sunkiomis nusikalstamomis veikomis, didelės žalos visuomenės saugumui prevencijos ir *a fortiori* nacionalinio saugumo užtikrinimo tikslai, atsižvelgiant į jų svarbą, kiek tai susiję su ankstesniame punkte primintomis *Cour constitutionnelle* (Konstitucinis Teismas) nurodytomis pareigomis veikti, gali pateisinti ypač didelius suvaržymus, kuriuos lemia tikslinis srauto ir vietos nustatymo duomenų saugojimas.

147 Taigi, kaip jau yra nusprendęs Teisingumo Teismas, Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, nedraudžia valstybei narei priimti teisės aktų, pagal kuriuos prevenciškai leidžiamas tikslinis srauto ir vietos nustatymo duomenų saugojimas kovos su sunkiomis nusikalstamomis veikomis, didelės grėsmės visuomenės saugumui prevencijos tikslais ir siekiant užtikrinti nacionalinį saugumą, su sąlyga, kad duomenų saugojimas, kiek tai susiję su saugotinų duomenų kategorijomis, konkrečiomis ryšio priemonėmis, duomenų subjektais ir numatyta saugojimo trukme, būtų apribotas tuo, kas griežtai būtina (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 108 punktą).

148 Tokios duomenų saugojimo priemonės ribos gali būti nustatytos, be kita ko, atsižvelgiant į duomenų subjektų kategorijas, nes pagal Direktyvos 2002/58 15 straipsnio 1 dalį nedraudžiami teisės aktai, grindžiami objektyviais kriterijais, leidžiančiais nustatyti asmenis, kurių srauto ir vietos nustatymo duomenys gali bent netiesiogiai atskleisti ryšį su sunkiomis nusikalstamomis veikomis, vienaip ar kitaip prisidėti prie kovos su sunkiomis nusikalstamomis veikomis arba užkirsti kelią didelio pavojaus visuomenės saugumui ar nacionaliniam saugumui atsiradimui (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 111 punktą).

149 Šiuo klausimu reikia patikslinti, kad tokie asmenys gali būti, be kita ko, tie, kurie per taikomas nacionalines procedūras ir remiantis objektyviais įrodymais iš anksto buvo nustatyti kaip keliantys grėsmę visuomenės saugumui arba atitinkamos valstybės narės nacionaliniam saugumui.

150 Srauto ir vietos nustatymo duomenų saugojimą numatančios priemonės ribos taip pat gali būti grindžiamos geografiniu kriterijumi, kai kompetentingos nacionalinės institucijos, remdamosi objektyviais ir nediskriminaciniais veiksniais, mano, kad vienoje ar keliose geografinėse teritorijose yra didelė rizika, kad bus rengiami ar vykdomi sunkūs nusikaltimai (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 111 punktą). Tokios zonos gali būti, be kita ko, vietos, kuriose įvykdoma daug sunkių nusikalstamų veikų, vietos, kuriose ypač susiduriama su sunkių nusikalstamų veikų vykdymo grėsme, pavyzdžiui, vietos ar infrastruktūra, kurias reguliariai lanko labai daug asmenų, arba strateginės vietos, pavyzdžiui, oro uostai, stotys ar rinkliavos zonos.

151 Siekiant užtikrinti, kad suvaržymas, kurį lemia tikslinio duomenų saugojimo priemonės, aprašytos šio sprendimo 147–150 punktuose, atitiktų proporcingumo principą, tokių priemonių trukmė negali viršyti to, kas griežtai būtina atsižvelgiant į siekiamą tikslą ir jas pateisinančias aplinkybes, nedarant poveikio galimam pratęsimui, kai išlieka būtinybė užtikrinti tokį duomenų saugojimą.

– Dėl teisėkūros priemonių, numatančių prevencinį IP adresų ir civilinės tapatybės duomenų saugojimą, siekiant kovoti su nusikalstamumu ir užtikrinti visuomenės saugumą

152 Reikia pažymėti, kad IP adresai, nors ir priskiriami prie srauto duomenų sugeneruojami nesiejant jų su konkrečiu pranešimu ir iš esmės tarpininkaujant elektroninių ryšių paslaugų teikėjams yra skirti identifikuoti fiziniam asmeniui, kuriam priklauso galinis įrenginys, iš kurio siunčiamas pranešimas internetu. Taigi elektroninio pašto ir interneto telefonijos srityje, jeigu išsaugomi tik ryšio šaltinio IP

adresai, o ne jo adresato adresai, tokie adresai savaime neatskleidžia informacijos apie trečiuosius asmenis, kurie kontaktavo su komunikaciją inicijavusiu asmeniu. Taigi šios kategorijos duomenys yra mažiau jautrūs nei kiti srauto duomenys.

153 Vis dėlto, kadangi IP adresai gali būti naudojami, be kita ko, išsamiai atsekti interneto vartotojo naršymo kelius, taigi ir jo veiklą internete, šie duomenys leidžia nustatyti išsamų šio vartotojo profilį. Taigi tokiam atsekimui reikalingų IP adresų saugojimas ir analizė yra didelis pagrindinių interneto vartotojo teisių, įtvirtintų Chartijos 7 ir 8 straipsniuose, suvaržymas, galintis turėti tokį atgrasomąjį poveikį, koks nurodytas šio sprendimo 118 punkte.

154 Siekiant suderinti nagrinėjamas teises ir interesus, kaip reikalaujama pagal šio sprendimo 130 punkte nurodytą jurisprudenciją, reikia atsižvelgti į tai, kad tuo atveju, kai nusikalstama veika padaryta internete, IP adresas gali būti vienintelė tyrimo priemonė, leidžianti nustatyti asmenį, kuriam šis adresas buvo suteiktas šios nusikalstamos veikos padarymo metu. Be to, elektroninių ryšių paslaugų teikėjų atliekamas IP adresų saugojimas, pasibaigus šių duomenų suteikimo terminui, iš esmės nėra būtinas išrašant sąskaitas už nagrinėjamas paslaugas, todėl, kaip Teisingumo Teismui pateiktose pastabose nurodė kelios vyriausybės, gali būti neįmanoma nustatyti internete padarytų nusikalstamų veikų, nesiremiant teisėkūros priemone pagal Direktyvos 2002/58 15 straipsnio 1 dalį. Taip, be kita ko, gali būti, kaip teigia šios vyriausybės, ypač sunkių nusikaltimų, susijusių su vaikų pornografija, kaip antai vaikų pornografijos, kaip tai suprantama pagal 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvos 2011/93/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR (OL L 335, 2011, p. 1 ir klaidų ištaisymas OL L 18, 2012, p. 7), 2 straipsnio c punktą, įsigijimo, sklaidos, perdavimo arba pateikimo internetu atveju.

155 Šiomis aplinkybėmis tiesa, kad teisėkūros priemonė, kuria numatyta saugoti visų fizinių asmenų, turinčių galinį įrenginį, iš kurio gali būti suteikta prieiga prie interneto, IP adresus, iš tiesų apima asmenis, kurie iš pirmo žvilgsnio nėra susiję, kaip tai suprantama pagal šio sprendimo 133 punkte nurodytą jurisprudenciją, su siekiamais tikslais, ir kad interneto vartotojai, atsižvelgiant į tai, kas konstatuota šio sprendimo 109 punkte, turi teisę pagal Chartijos 7 ir 8 straipsnius tikėtis, kad jų tapatybė nebus iš principo atskleista, tačiau teisėkūros priemonė, numatanti bendrą ir nediferencijuotą prisijungimo šaltinio IP adresų saugojimą, iš esmės nėra prieštaraujanti Direktyvos 2002/58 15 straipsnio 1 daliai, siejamai su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, jeigu ji taikoma griežtai laikantis materialinių ir procedūrinių sąlygų, reglamentuojančių šių duomenų naudojimą.

156 Atsižvelgiant į Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymo dydį, šį suvaržymą gali pateisinti tik kova su sunkiais nusikaltimais, didelės grėsmės visuomenės saugumui prevencija bei siekis užtikrinti nacionalinį saugumą. Be to, duomenų saugojimo trukmė negali viršyti to, kas griežtai būtina atsižvelgiant į siekiamą tikslą. Galiausiai tokia priemone turi būti numatytos griežtos šių duomenų naudojimo sąlygos ir garantijos, be kita ko, taikant atsekimą, kiek tai susiję su duomenų subjektų pranešimais ir veikla internete.

157 Galiausiai, kalbant apie duomenis, susijusius su elektroninių ryšių priemonių naudotojų civiline tapatybe, pažymėtina, kad iš šių duomenų neįmanoma sužinoti pranešimų datos, laiko, trukmės ir gavėjų, taip pat vietų, iš kurių siųsti šie pranešimai, arba pranešimų tam tikriems asmenims dažnumo per tam tikrą laikotarpį, todėl, be jų kontaktinių duomenų, pavyzdžiui, adresų, tokie duomenys neteikia jokios informacijos apie išsiųstus pranešimu, taigi ir apie privatų gyvenimą. Vadinasi, suvaržymas, kurį lemia šių duomenų saugojimas, iš principo negali būti laikomas dideliu (šiuo klausimu žr. 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 59 ir 60 punktus).

158 Iš to matyti, kad, atsižvelgiant į tai, kas išdėstyta šio sprendimo 140 punkte, teisėkūros priemonės, skirtos tokiems duomenims tvarkyti, be kita ko, jiems saugoti ir prieigai prie jų, siekiant tik nustatyti atitinkamo naudotojo tapatybę, kai šie duomenys negali būti siejami su pranešimų informacija, gali

būti pateisinamos nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslu apskritai, nurodytu Direktyvos 2002/58 15 straipsnio 1 dalies pirmame sakinyje (šiuo klausimu žr. 2018 m. spalio 2 d. Sprendimo *Ministerio Fiscal*, C-207/16, EU:C:2018:788, 62 punktą).

159 Tokiomis aplinkybėmis, atsižvelgiant į būtinybę suderinti nagrinėjamas teises ir interesus, ir dėl šio sprendimo 131 ir 158 punktuose nurodytų priežasčių reikia konstatuoti, kad, nesant ryšio tarp visų elektroninių ryšių priemonių naudotojų ir siekiamų tikslų, pagal Direktyvos 2002/58 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, nedraudžiama teisėkūros priemonė, elektroninių ryšių paslaugų teikėjams nustatanti pareigą be konkretaus termino saugoti visų elektroninių ryšių priemonių naudotojų civilinės tapatybės nustatymo duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ir baudžiamojo persekiojimo tikslais, taip pat siekiant užtikrinti visuomenės saugumą, nereikalaujant, kad nusikalstamos veikos arba grėsmės visuomenės saugumui ar jo pažeidimai būtų sunkūs.

– Dėl teisėkūros priemonių, numatančių operatyvų srauto ir vietos nustatymo duomenų saugojimą, siekiant kovoti su sunkiomis nusikalstamomis veikomis

160 Dėl srauto ir vietos nustatymo duomenų, kuriuos elektroninių ryšių paslaugų teikėjai tvarko ir saugo, remdamiesi Direktyvos 2002/58 5, 6 ir 9 straipsniais arba teisėkūros priemonėmis, priimtomis pagal šios direktyvos 15 straipsnio 1 dalį, kaip antai aprašytomis šio sprendimo 134–159 punktuose, pažymėtina, kad šie duomenys, atsižvelgiant į konkretų atvejį, iš principo turi būti ištrinti arba anoniminti pasibaigus teisės aktuose nustatytiems terminams, per kuriuos jie turi būti tvarkomi ar saugomi pagal šią direktyvą perkeliančias nacionalinės teisės nuostatas.

161 Vis dėlto atliekant tokį tvarkymą ir saugojimą gali susiklostyti situacijos, kai kyla būtinybė saugoti šiuos duomenis ilgiau, nei numatyti terminai, siekiant išaiškinti sunkias nusikalstamas veikas arba nacionalinio saugumo pažeidimus; taip gali būti tiek tuo atveju, kai šios nusikalstamos veikos ar žala jau yra nustatytos, tiek tuo atveju, kai, objektyviai išnagrinėjus visas svarbias aplinkybes, gali būti pagrįstai įtariamas jų egzistavimas.

162 Šiuo klausimu reikia pažymėti, kad 2001 m. lapkričio 23 d. Europos Tarybos konvencijos dėl elektroninių nusikaltimų (Europos sutarčių serija, Nr. 185), kurią pasirašė 27 valstybės narės, o ratifikavo 25 iš jų, ir kurios tikslas – palengvinti kovą su nusikalstamomis veikomis, padarytomis per kompiuterinius tinklus, 14 straipsnyje numatyta, kad atlikdamos tyrimus ar vykstant specifiniams baudžiamiesiems procesams susitariančiosios šalys imasi tam tikrų priemonių dėl tokių saugomų srauto duomenų, pavyzdžiui, operatyviai saugo šiuos duomenis. Konkrečiai kalbant, šios konvencijos 16 straipsnio 1 dalyje nustatyta, kad susitariančiosios šalys priima tokius teisės aktus ir kitas priemones, kurios yra būtinos, kad jų kompetentingos institucijos galėtų nurodyti arba kitaip įpareigoti operatyviai saugoti srauto duomenis, laikomus kompiuterinėje sistemoje, ypač kai yra pagrindo manyti, jog šie duomenys gali būti nesunkiai prarasti arba pakeisti.

163 Esant tokiai situacijai, kokia nurodyta šio sprendimo 161 punkte, valstybės narės, atsižvelgdamos į būtiną nagrinėjamų teisių ir interesų suderinimą, nurodytą šio sprendimo 130 punkte, gali pagal Direktyvos 2002/58 15 straipsnio 1 dalį priimtuose teisės aktuose numatyti galimybę kompetentingos institucijos, kuriai taikoma veiksminga teisminė kontrolė, sprendimu įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų saugojimą.

164 Tiek, kiek tokio operatyvaus saugojimo tikslas neatitinka tikslo, dėl kurio duomenys buvo surinkti ir saugomi iš pradžių, ir tiek, kiek bet koks duomenų tvarkymas pagal Chartijos 8 straipsnio 2 dalį turi atitikti apibrėžtus tikslus, valstybės narės savo teisės aktuose turi nurodyti tikslą, dėl kurio galima operatyviai saugoti duomenis. Atsižvelgiant į Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymo, kurį gali sukelti toks saugojimas, dydį, šį suvaržymą galima pateisinti tik kova su sunkiais

nusikaltimais ir *a fortiori* nacionalinio saugumo užtikrinimu. Be to, siekiant užtikrinti, kad suvaržymas, kurį lemia tokios rūšies priemonė, neviršytų to, kas griežtai būtina, pirma, reikia, kad įpareigojimas saugoti duomenis būtų taikomas tik srauto ir vietos nustatymo duomenims, galintiems padėti išaiškinti sunkią nusikalstamą veiką ar atitinkamą grėsmę nacionaliniam saugumui. Antra, duomenų saugojimo trukmė turi būti apribota tuo, kas griežtai būtina, tačiau ji gali būti pratęsta, jei tai pateisinama šios priemonės aplinkybėmis ir tikslu.

165 Šiuo klausimu svarbu pažymėti, kad toks operatyvus saugojimas neturi apimti tik asmenų, kurie konkrečiai įtariami padarę nusikalstamą veiką ar kelia grėsmę nacionaliniam saugumui, duomenų. Laikantis Direktyvos 2002/58 15 straipsnio 1 dalyje, siejamoje su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, nustatytų pagrindų ir remiantis tuo, kas išdėstyta šio sprendimo 133 punkte, tokia priemonė, atsižvelgiant į teisės aktų leidėjo pasirinkimą ir laikantis to, kas griežtai būtina, gali apimti kitų asmenų nei tie, kurie įtariami planavę arba padarę sunkią nusikalstamą veiką ar keliantys grėsmę nacionaliniam saugumui, srauto ir vietos nustatymo duomenis, jeigu šie duomenys, remiantis objektyviais ir nediskriminaciniais veiksniais, gali padėti išaiškinti tokią nusikalstamą veiką ar grėsmę nacionaliniam saugumui; tai gali būti, pavyzdžiui, tokios nusikalstamos veikos aukos, jos socialinės ar profesinės aplinkos duomenys arba tam tikros geografinės zonos, pavyzdžiui, nusikalstamos veikos ar grėsmės nacionaliniam saugumui rengimo ar vykdymo vietos duomenys. Be to, kompetentingų institucijų prieiga prie taip saugomų duomenų turi būti užtikrinama laikantis jurisprudencijoje, kurioje aiškinama Direktyva 2002/58, numatytų sąlygų (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 118–121 punktus ir juose nurodytą jurisprudenciją).

166 Taip pat reikia pridurti, kad, kaip matyti visų pirma iš šio sprendimo 115 ir 133 punktų, prieiga prie teikėjų saugomų srauto ir vietos nustatymo duomenų taikant priemonę, kurios imtasi pagal Direktyvos 2002/58 15 straipsnio 1 dalį, iš esmės gali būti pateisinama tik bendrojo intereso tikslu, dėl kurio šiems teikėjams nustatytas įpareigojimas saugoti duomenis. Konkrečiai kalbant, darytina išvada, kad prieiga prie tokių duomenų, siekiant patraukti atsakomybėn už nekvalifikuotą nusikalstamą veiką ir taikyti sankciją už ją, jokiu būdu negali būti suteikta, jei tokių duomenų saugojimas pateisinamas kovos su sunkiais nusikaltimais arba *a fortiori* nacionalinio saugumo užtikrinimo tikslu. Vis dėlto pagal proporcingumo principą, kaip nurodyta šio sprendimo 131 punkte, prieiga prie duomenų, saugomų siekiant kovoti su sunkiais nusikaltimais, jeigu laikomasi ankstesniame punkte nurodytų materialinių ir procedūrinių sąlygų, susijusių su tokia prieiga, gali būti pateisinama nacionalinio saugumo užtikrinimo tikslu.

167 Šiuo klausimu valstybės narės savo teisės aktuose gali numatyti, kad prieiga prie srauto ir vietos nustatymo duomenų gali, laikantis tų pačių materialinių ir procesinių sąlygų, būti suteikta siekiant kovoti su sunkiomis nusikalstamomis veikomis arba užtikrinti nacionalinį saugumą, kai šiuos duomenis saugo paslaugų teikėjas, laikantis Direktyvos 2002/58 5, 6 ir 9 straipsnių arba 15 straipsnio 1 dalies.

168 Atsižvelgiant į visa tai, kas išdėstyta, į pirmuosius klausimus bylose C-511/18 ir C-512/18, taip pat į pirmąjį ir antrąjį klausimus byloje C-520/18 reikia atsakyti, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiamos teisėkūros priemonės, kuriomis, siekiant šio 15 straipsnio 1 dalyje numatytų tikslų, prevenciškai numatomas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas. Vis dėlto pagal minėto 15 straipsnio 1 dalį, siejamą su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, nedraudžiamos tokios teisėkūros priemonės:

– kuriomis, siekiant užtikrinti nacionalinį saugumą, leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant saugoti srauto ir vietos nustatymo duomenis tais atvejais, kai atitinkama valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra, esama arba numatoma, o sprendimui, kuriame nustatytas toks įpareigojimas, gali būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią,

kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi sąlygų ir garantijų, kurios turi būti numatytos; toks įpareigojimas gali būti nustatytas tik laikotarpiui, neviršijančiam to, kas griežtai būtina, bet jeigu grėsmė išlieka, galimam pratęsti;

– kuriomis, siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiomis nusikalstamomis veikomis ir užkirsti kelią didelei grėsmei visuomenės saugumui, numatomas tikslinis srauto ir vietos nustatymo duomenų saugojimas, kuris, remiantis objektyviais ir nediskriminaciniais veiksniais, atsižvelgiant į duomenų subjektų kategorijas arba geografinius kriterijus, būtų apribotas laikotarpio, neviršijančio to, kas griežtai būtina, tačiau kurį galima pratęsti;

– kuriomis, siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiomis nusikalstamomis veikomis ir užkirsti kelią didelei grėsmei visuomenės saugumui, numatomas bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas laikotarpiu, neviršijančiu to, kas griežtai būtina;

– kuriomis, siekiant užtikrinti nacionalinį saugumą, kovoti su nusikalstamumu ir užtikrinti visuomenės saugumą, numatomas bendras ir nediferencijuotas duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas ir

– kuriomis, siekiant kovoti su sunkiomis nusikalstamomis veikomis ir *a fortiori* užtikrinti nacionalinį saugumą, leidžiama kompetentingos institucijos, kuriai taikoma veiksminga teisminė kontrolė, sprendimu įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų, kuriuos turi šie paslaugų teikėjai, saugojimą,

kai tokios priemonės aiškiomis ir tiksliomis taisyklėmis užtikrina, kad saugant nagrinėjamus duomenis būtų laikomasi su tokiu saugojimu susijusių materialinių ir procesinių sąlygų ir atitinkami asmenys turėtų veiksmingas garantijas nuo piktnaudžiavimo rizikos.

Dėl antrojo ir trečiojo klausimų byloje C-511/18

169 Antruoju ir trečiuoju klausimais byloje C-511/18 prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiami nacionalinės teisės aktai, kuriais elektroninių ryšių paslaugų teikėjai įpareigojami savo tinkluose įgyvendinti priemones, leidžiančias, pirma, atlikti automatizuotą srauto ir vietos nustatymo duomenų analizę ir šių duomenų rinkimą realiuoju laiku ir, antra, realiuoju laiku rinkti techninius duomenis, susijusius su naudojamų galinių įrenginių vieta, nereikalaujant informuoti duomenų subjektų apie tokį duomenų tvarkymą ir rinkimą.

170 Prašymą priimti prejudicinį sprendimą pateikęs teismas patikslina, kad informacijos rinkimo metodai, numatyti CSI L. 851-2–L. 851-4 straipsniuose, nereiškia, kad elektroninių ryšių paslaugų teikėjams taikomas specifinis reikalavimas saugoti srauto ir vietos nustatymo duomenis. Konkrečiai dėl CSI L. 851-3 straipsnyje nurodytos automatizuotos analizės tas teismas pažymi, kad šio tvarkymo tikslas – remiantis šiam tikslui apibrėžtais kriterijais nustatyti ryšius, galinčius atskleisti terorizmo grėsmę. Minėtas teismas konstatuoja, kad CSI L. 851-2 straipsnyje numatytas duomenų rinkimas realiuoju laiku susijęs tik su vienu ar daugiau asmenų, kurie iš anksto buvo nustatyti kaip galintys turėti sąsają su terorizmo grėsme. To paties teismo teigimu, šie du būdai gali būti naudojami tik terorizmo prevencijos tikslais ir yra susiję su CSI L. 851-1 ir R. 851-5 straipsniuose nurodytais duomenimis.

171 Pirmiausia reikia pažymėti, jog aplinkybė, kad pagal CSI L. 851-3 straipsnį jame numatyta automatizuota analizė savaime neleidžia nustatyti naudotojų, kurių duomenys pateikiami šiai analizei, tapatybės, netrukdo kvalifikuoti tokių duomenų kaip „asmens duomenų“. Kadangi šios nuostatos IV punkte numatyta procedūra vėlesniame etape leidžia nustatyti asmens ar asmenų, susijusių su duomenimis, kurių automatizuota analizė parodė, kad tokie asmenys gali kelti terorizmo grėsmę,

tapatybę, visų asmenų, kurių duomenys analizuojami automatizuotai, tapatybė gali būti nustatyta remiantis šiais duomenimis. Pagal Reglamento 2016/679 4 straipsnio 1 punkte pateiktą asmens duomenų apibrėžtį tokie duomenys yra informacija, susijusi, be kita ko, su asmeniu, kurio tapatybė gali būti nustatyta.

Dėl automatizuotos srauto ir vietos nustatymo duomenų analizės

172 Iš CSI L. 851-3 straipsnio matyti, kad jame numatyta automatizuota analizė iš esmės atitinka visų elektroninių ryšių paslaugų teikėjų saugomų srauto ir vietos nustatymo duomenų filtravimą, atliekamą kompetentingų nacionalinių institucijų prašymu ir taikant jų nustatytus parametrus. Darytina išvada, kad visi elektroninių ryšių priemonių naudotojų duomenys tikrinami, jei atitinka šiuos parametrus. Taigi reikia pripažinti, kad tokia automatizuota analizė reiškia, kad atitinkami elektroninių ryšių paslaugų teikėjai kompetentingos institucijos vardu turi atlikti bendrą ir nediferencijuotą tvarkymą, naudojant automatizuotą procesą, kaip tai suprantama pagal Reglamento 2016/679 4 straipsnio 2 punktą, apimantį visų elektroninių ryšių priemonių naudotojų srauto ir vietos nustatymo duomenis. Šis tvarkymas nepriklauso nuo paskesnio duomenų apie asmenis, identifikuotus atlikus automatizuotą analizę, rinkimo, leistino pagal CSI L. 851-3 straipsnio IV dalį.

173 Nacionalinės teisės aktais, pagal kuriuos leidžiama atlikti tokią automatizuotą srauto ir vietos nustatymo duomenų analizę, nukrypstama nuo Direktyvos 2002/58 5 straipsnyje nustatytos pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą. Tokie teisės aktai taip pat suvaržo Chartijos 7 ir 8 straipsniuose įtvirtintas pagrindines teises, neatsižvelgiant į vėlesnį šių duomenų panaudojimą. Galiausiai, remiantis šio sprendimo 118 punkte nurodyta jurisprudencija, minėti teisės aktai gali atgrasyti naudotis Chartijos 11 straipsnyje įtvirtinta saviraiškos laisve.

174 Be to, suvaržymas, kurį lemia automatizuota srauto ir vietos nustatymo duomenų analizė, kaip antai nagrinėjama pagrindinėje byloje, yra ypač didelis, nes juo bendrai ir nediferencijuojant apimami elektroninių ryšių priemones naudojančių asmenų duomenys. Tokia išvada juo labiau darytina, kai, kaip matyti iš pagrindinėje byloje nagrinėjamų nacionalinės teisės aktų, duomenys, kurie yra automatizuotos analizės objektas, gali atskleisti internete naršytos informacijos pobūdį. Be to, tokia automatizuota analizė taikoma bendrai visiems asmenims, naudojantiems elektroninių ryšių priemones, taigi ir tiems, dėl kurių nėra jokių požymių, leidžiančių manyti, kad jų elgesys gali turėti bent netiesioginį ar tolimą ryšį su teroristine veikla.

175 Dėl tokio suvaržymo pateisinimo reikia patikslinti, jog Chartijos 52 straipsnio 1 dalyje numatytas reikalavimas, kad bet koks pagrindinių teisių įgyvendinimo apribojimas būtų numatytas įstatyme, reiškia, kad pačiame teisiniame pagrinde, kuriuo leidžiamas šių teisių suvaržymas, būtų apibrėžta atitinkamos teisės įgyvendinimo apribojimo apimtis (šiuo klausimu žr. 2020 m. liepos 16 d. Sprendimo *Facebook Ireland ir Schrems*, C-311/18, EU:C:2020:559, 175 punktą ir jame nurodytą jurisprudenciją).

176 Be to, tam, kad būtų įvykdytas šio sprendimo 130 ir 131 punktuose primintas proporcingumo reikalavimas, pagal kurį nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neturi viršyti to, kas yra griežtai būtina, nacionalinės teisės aktai, reglamentuojantys kompetentingų institucijų prieigą prie saugomų srauto ir vietos nustatymo duomenų, turi atitikti reikalavimus, kylančius iš šio sprendimo 132 punkte nurodytos jurisprudencijos. Konkrečiai kalbant, tokiuose teisės aktuose negali būti apsiribojama reikalavimu, kad valdžios institucijų prieiga prie duomenų atitiktų šiuo teisės aktu siekiamą tikslą; juose taip pat turi būti numatytos tokį naudojimą reglamentuojančios materialinės ir procesinės sąlygos (pagal analogiją žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 192 punktą ir jame nurodytą jurisprudenciją).

177 Šiuo klausimu reikia priminti, kad labai didelis suvaržymas, kurį lemia bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas, nurodytas šio sprendimo 134–139 punktuose pateiktuose argumentuose, ir labai didelis suvaržymas, kurį lemia tokių duomenų automatizuota analizė, gali atitikti proporcingumo reikalavimą tik tais atvejais, kai valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra ir esama arba numatoma, su sąlyga, kad tokio saugojimo trukmė būtų apribota tuo, kas griežtai būtina.

178 Pirmesniame šio sprendimo punkte nurodytais atvejais automatizuotos visų elektroninių ryšių priemonių naudotojų srauto ir vietos nustatymo duomenų analizės atlikimas griežtai ribotą laikotarpį gali būti laikomas pateisinamu, atsižvelgiant į reikalavimus, kylančius iš Direktyvos 2002/58 15 straipsnio 1 dalies, siejamos su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi.

179 Taigi siekiant užtikrinti, kad tokios priemonės taikymas iš tikrųjų apsiribotų tuo, kas griežtai būtina nacionaliniam saugumui užtikrinti, ir, konkrečiai kalbant, terorizmo prevencijai, svarbu, kad, atsižvelgiant į tai, kas konstatuota šio sprendimo 139 punkte, sprendimui, kuriuo leidžiama atlikti automatizuotą analizę, galėtų būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, kad būtų patikrinta, ar egzistuoja minėtą priemonę pateisinanti situacija ir ar laikomasi sąlygų ir garantijų, kurios turi būti nustatytos.

180 Šiuo klausimu reikia pažymėti, kad iš anksto nustatyti būdai ir kriterijai, kuriais grindžiamas toks duomenų tvarkymas, turi būti, pirma, konkretūs ir patikimi, leidžiantys nustatyti asmenų, kurie gali kelti pagrįstą įtarimą dėl dalyvavimo teroristinėse nusikalstamose veikose, tapatybę ir, antra, nediskriminuojantys (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 172 punktą).

181 Taip pat svarbu priminti, kad bet kokia automatizuota analizė, atliekama taikant būdus ir kriterijus, grindžiamus prielaida, kad asmens rasinė ar etninė kilmė, politinės pažiūros, religiniai ar filosofiniai įsitikinimai, priklausymas profesinei sąjungai, sveikatos būklė ar seksualinis gyvenimas gali būti savaime reikšmingi terorizmo prevencijai, neatsižvelgiant į individualų asmens elgesį, pažeidžia Chartijos 7 ir 8 straipsniuose, siejamuose su jos 21 straipsniu, užtikrinamas teises. Taigi būdai ir kriterijai, iš anksto nustatyti siekiant atlikti automatizuotą analizę, skirtą užkirsti keliui teroristinėms veikoms, keliančioms didelę grėsmę nacionaliniam saugumui, negali būti grindžiami vien šiais jautriais duomenimis (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 165 punktą).

182 Be to, automatizuota srauto ir vietos nustatymo duomenų analizė neišvengiamai gali lemti tam tikrų klaidų, todėl bet koks po automatizuoto tvarkymo gautas teigiamas rezultatas turi būti individualiai patikrintas neautomatizuotomis priemonėmis prieš imantis individualios priemonės, kuri turėtų neigiamą poveikį duomenų subjektams, kaip antai nustatant paskesnį srauto ir vietos nustatymo duomenų rinkimą realiuoju laiku, nes tokia priemonė negali būti galutinai grindžiama vien automatizuoto tvarkymo rezultatu. Be to, siekiant praktiškai užtikrinti, kad iš anksto nustatyti būdai ir kriterijai, jų naudojimas ir naudojamos duomenų bazės nebūtų diskriminacinio pobūdžio ir neviršytų to, kas griežtai būtina, atsižvelgiant į tikslą užkirsti kelią teroristinei veiklai, keliančiai didelę grėsmę nacionaliniam saugumui, tokių iš anksto nustatytų būdų ir kriterijų bei naudojamų duomenų bazių patikimumas ir aktualumas turi būti reguliariai peržiūrimi (šiuo klausimu žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 165 punktą).

Dėl srauto ir vietos nustatymo duomenų rinkimo realiuoju laiku

183 CSI L. 851-2 straipsnyje numatytas srauto ir vietos nustatymo duomenų rinkimas realiuoju laiku gali būti leidžiamas individualiai, kiek tai susiję su „iš anksto identifikuotu asmeniu, kuris gali būti susijęs su [terorizmo] grėsme“. Be to, pagal šią nuostatą, „kai yra rimtų priežasčių manyti, kad vienas ar keli

asmenys, susiję su asmens, dėl kurio išduotas leidimas, aplinka, gali pateikti informaciją dėl tikslo, kuriuo remiantis išduotas leidimas, toks leidimas gali būti išduodamas individualiai dėl kiekvieno iš šių asmenų“.

184 Duomenys, kuriems taikoma tokia priemonė, leidžia kompetentingoms nacionalinėms institucijoms leidimo galiojimo laikotarpiu nuolat ir realiuoju laiku stebėti kontaktinius asmenis, su kuriais duomenų subjektai bendrauja, kokiomis priemonėmis jie bendrauja, jų komunikacijos trukmę, gyvenamąsias vietas ir judėjimą. Be to, atrodo, jie gali atskleisti internete naršytos informacijos pobūdį. Kaip matyti iš šio sprendimo 117 punkto, šie duomenys, vertinami kaip visuma, leidžia daryti labai tikslias išvadas dėl duomenų subjektų privataus gyvenimo ir nustatyti jų profilį – tokia informacija, kiek tai susiję su teise į privataus gyvenimo gerbimą, yra tokia pat jautri kaip ir pats pranešimų turinys.

185 Kalbant apie CSI L. 851-4 straipsnyje numatytą duomenų rinkimą realiuoju laiku, pažymėtina, kad pagal šią nuostatą leidžiama rinkti techninius duomenis apie galinių įrenginių vietą ir realiuoju laiku juos perduoti Ministro Pirmininko tarnybai. Taigi tokie duomenys leidžia kompetentingai tarnybai bet kuriuo momentu leidimo galiojimo laikotarpiu nuolat ir realiuoju laiku nustatyti naudojamos galinės įrangos, pavyzdžiui, mobiliųjų telefonų, vietą.

186 Nacionalinės teisės aktais, pagal kuriuos leidžiamas toks duomenų rinkimas realiuoju laiku, kaip ir teisės aktais, kuriais leidžiama automatizuota duomenų analizė, nukrypstama nuo Direktyvos 2002/58 5 straipsnyje nustatytos pagrindinės pareigos užtikrinti elektroninių ryšių ir su jais susijusių duomenų konfidencialumą. Taigi jie taip pat laikomi Chartijos 7 ir 8 straipsniuose įtvirtintų pagrindinių teisių suvaržymu ir gali atgrasyti naudotis Chartijos 11 straipsnyje garantuojama saviraiškos laisve.

187 Reikia pabrėžti, kad suvaržymas, susijęs su duomenų, leidžiančių nustatyti galinio įrenginio vietą, rinkimu realiuoju laiku, yra ypač didelis, nes šie duomenys kompetentingoms nacionalinėms institucijoms suteikia galimybę tiksliai ir nuolat stebėti mobiliųjų telefonų naudotojų judėjimą. Kadangi šiuos duomenis reikia laikyti ypač jautriais, kompetentingų valdžios institucijų prieigą prie tokių duomenų realiuoju laiku reikia skirti nuo prieigos prie jų nerealiuoju metu; pirmoji prieiga yra labiau suvaržanti, nes leidžia labai tiksliai stebėti šiuos naudotojus (kiek tai susiję su EŽTK 8 straipsniu, pagal analogiją žr. 2018 m. vasario 8 d. EŽTT sprendimo *Ben Faiza prieš Prancūziją*, CE:ECHR:2018:0208JUD003144612, 74 punktą). Be to, šio ribojimo intensyvumas padidėja, kai duomenų rinkimas realiuoju laiku apima ir duomenų subjektų srauto duomenis.

188 Nors pagrindinėje byloje nagrinėjamais nacionalinės teisės aktais siekiamas terorizmo prevencijos tikslas, atsižvelgiant į jo svarbą, gali pateisinti suvaržymą, susijusį su srauto ir vietos nustatymo duomenų rinkimu realiuoju laiku, tokia priemonė, atsižvelgiant į ypač ribojamąjį jos pobūdį, gali būti įgyvendinta tik dėl asmenų, dėl kurių yra pagrįsta priežastis įtarti, kad jie vienaip ar kitaip susiję su terorizmo veikla. Prieiga prie asmenų, kurie nepriklauso šiai kategorijai, duomenų gali būti taikoma tik nerealiuoju laiku ir, remiantis Teisingumo Teismo jurisprudencija, tik ypatingais atvejais, kaip antai susijusiais su terorizmo veikla, kai yra objektyvių veiksnių, leidžiančių manyti, kad konkrečiu atveju šie duomenys galėtų veiksmingai prisidėti prie kovos su terorizmu (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 119 punktą ir jame nurodytą jurisprudenciją).

189 Be to, sprendimas leisti realiuoju laiku rinkti srauto ir vietos nustatymo duomenis turi būti grindžiamas objektyviais nacionalinės teisės aktuose numatytais kriterijais. Konkrečiai kalbant, remiantis šio sprendimo 176 punkte nurodyta jurisprudencija, šiuose teisės aktuose turi būti apibrėžtos aplinkybės ir sąlygos, kuriomis toks duomenų rinkimas gali būti leidžiamas, ir numatyta, kad, kaip nurodyta pirmesniame šio sprendimo punkte, jis gali būti susiję tik su asmenimis, dėl kurių gali būti nustatytas ryšys su terorizmo prevencijos tikslu. Be to, sprendimas leisti realiuoju laiku rinkti srauto ir vietos nustatymo duomenis turi būti grindžiamas objektyviais ir nediskriminaciniais kriterijais, numatytais

nacionalinės teisės aktuose. Siekiant praktiškai užtikrinti, kad būtų laikomasi šių sąlygų, labai svarbu, kad priemonės, pagal kurią duomenys būtų renkami realiuoju laiku, įgyvendinimo kontrolę iš anksto atliktų teismas arba nepriklausoma administracinė institucija, kurios sprendimas turi privalomąją galią, o šis teismas ar institucija, be kita ko, turi įsitikinti, kad toks duomenų rinkimas realiuoju laiku leidžiamas tik tiek, kiek tai griežtai būtina (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 120 punktą). Tinkamai pagrįstos skubos atveju kontrolė turi būti vykdoma per trumpą laiką.

Dėl informacijos teikimo asmenims, kurių duomenys buvo surinkti ar išanalizuoti

190 Svarbu, kad kompetentingos nacionalinės institucijos, renkančios srauto ir vietos nustatymo duomenis realiuoju laiku, remdamosi taikytinomis nacionalinėmis procedūromis apie tai informuotų duomenų subjektus, jeigu (ir nuo to momento, kai) toks atskleidimas negali pakenkti šiai institucijai tenkančioms užduotims. Iš tiesų ši informacija yra būtina tam, kad šie asmenys galėtų pasinaudoti iš Chartijos 7 ir 8 straipsnių išplaukiančiomis teisėmis prašyti leisti susipažinti su savo asmens duomenimis, kuriems taikomos šios priemonės, ir prireikus juos ištaisyti ar pašalinti, taip pat pagal Chartijos 47 straipsnio pirmą pastraipą pasinaudoti veiksminga teisine gynyba teisme; tokia teisė, be kita ko, yra aiškiai užtikrinta Direktyvos 2002/58 15 straipsnio 2 dalyje, siejamoje su Reglamento 2016/679 79 straipsnio 1 dalimi (šiuo klausimu žr. 2016 m. gruodžio 21 d. Sprendimo *Tele2*, C-203/15 ir C-698/15, EU:C:2016:970, 121 punktą ir jame nurodytą jurisprudenciją; taip pat 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 219 ir 220 punktus).

191 Kalbant apie reikalaujamą pateikti informaciją atliekant automatizuotą srauto ir vietos nustatymo duomenų analizę, pažymėtina, kad kompetentinga nacionalinė institucija privalo paskelbti bendro pobūdžio informaciją, susijusią su šia analize, bet neprivalo individualiai informuoti duomenų subjektų. Tačiau, jei duomenys atitinka parametrus, kurie nurodyti priemonėje, leidžiančioje atlikti automatizuotą analizę, ir kai ši institucija nustato duomenų subjekto tapatybę, kad išsamiau išanalizuotų su juo susijusius duomenis, toks asmuo turi būti individualiai informuojamas. Vis dėlto tokia informacija turi būti pateikiama tik jeigu (ir nuo to momento, kai) toks atskleidimas negali pakenkti šiai institucijai tenkančioms užduotims (pagal analogiją žr. 2017 m. liepos 26 d. Nuomonės 1/15 (*ES ir Kanados PNR susitarimas*), EU:C:2017:592, 222–224 punktus).

192 Atsižvelgiant į visa tai, kas išdėstyta, į antrąjį ir trečiąjį klausimus byloje C-511/18 reikia atsakyti, kad Direktyvos 2002/58 15 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją nedraudžiamos nacionalinės teisės nuostatos, kuriomis elektroninių ryšių paslaugų teikėjai įpareigojami, pirma, vykdyti, be kita ko, srauto ir vietos nustatymo duomenų automatizuotą analizę bei jų rinkimą realiuoju laiku ir, antra, realiuoju laiku rinkti techninius duomenis, susijusius su galinių įrenginių vieta, jeigu:

– automatizuota analizė atliekama tik tais atvejais, kai valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra ir esama arba numatoma, o tokios analizės atlikimui turi būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja minėtą priemonę pateisinanti situacija ir ar laikomasi sąlygų ir garantijų, kurios turi būti nustatytos, ir jeigu

– srauto ir vietos nustatymo duomenų rinkimas realiuoju laiku taikomas tik tiems asmenims, dėl kurių yra pagrįsta priežastis įtarti, kad jie vienaip ar kitaip susiję su terorizmo veikla, ir jeigu tokiam duomenų rinkimui taikoma išankstinė teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant įsitikinti, kad toks duomenų rinkimas realiuoju laiku leidžiamas tik tiek, kiek tai griežtai būtina. Tinkamai pagrįstos skubos atveju kontrolė turi būti vykdoma per trumpą laiką.

Dėl antrojo klausimo byloje C-512/18

193 Antruoju klausimu byloje C-512/18 prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar Direktyvos 2000/31 nuostatos, siejamos su Chartijos 6–8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinamos taip, kad jomis draudžiami nacionalinės teisės aktai, kuriais prieigos prie visuomenei skirtų ryšių paslaugų internetu teikėjai ir prieglobos paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai saugoti, be kita ko, su šiomis paslaugomis susijusius asmens duomenis.

194 Teigdamas, kad tokios paslaugos patenka į Direktyvos 2000/31, o ne į Direktyvos 2002/58 taikymo sritį, prašymą priimti prejudicinį sprendimą pateikęs teismas mano, kad Direktyvos 2000/31 15 straipsnio 1 ir 2 dalyse, siejamose su jos 12 ir 14 straipsniais, nenustatytas principinis draudimas saugoti duomenis, susijusius su turinio sukūrimu, nuo kurio būtų galima nukrypti tik išimtiniais atvejais. Vis dėlto šiam teismui kyla klausimas, ar reikia vadovautis tokiu vertinimu, atsižvelgiant į tai, kad būtina paisyti Chartijos 6–8 ir 11 straipsniuose įtvirtintų pagrindinių teisių.

195 Be to, prašymą priimti prejudicinį sprendimą pateikęs teismas patikslina, kad jo klausimas susijęs su saugojimo pareiga, numatyta LCEN 6 straipsnyje, siejamame su Dekretu Nr. 2011-219. Duomenys, kuriuos šiuo tikslu turi saugoti atitinkami paslaugų teikėjai, apima, be kita ko, duomenis, susijusius su asmenų, kurie naudojasi šiomis paslaugomis, civiline tapatybe, kaip antai jų pavardes, vardus, adresus, susijusius pašto adresus, elektroninio pašto ar susijusios paskyros adresus, slaptažodžius ir naudotą mokėjimo būdą, kai sutarties sudarymas ar prisijungimas prie paskyros yra mokami, taip pat mokėjimo nuorodą, sumą ir sandorio datą bei laiką.

196 Be to, duomenys, kuriuos reikia saugoti, apima abonentų, jungčių ir naudotos galinės įrangos identifikatorius, turiniui priskirtus identifikatorius, prisijungimų datas, pradžios ir pabaigos laiką, taip pat protokolų, naudojamų prisijungti prie paslaugos ir turiniui perduoti, rūšis. Prieigos prie šių duomenų, kurių saugojimo trukmė yra vieni metai, galima prašyti vykstant baudžiamajam ir civiliniam procesams, siekiant, kad būtų laikomasi civilinės ar baudžiamosios atsakomybės taisyklių, taip pat taikant informacijos rinkimo priemones, kurioms taikomas CSI L. 851-1 straipsnis.

197 Šiuo klausimu reikia pažymėti, kad pagal Direktyvos 2000/31 1 straipsnio 2 dalį šia direktyva derinamos tam tikros nacionalinės nuostatos, taikomos šios direktyvos 2 straipsnio a punkte nurodytoms informacinės visuomenės paslaugoms.

198 Tokios paslaugos apima paslaugas, kurios teikiamos per atstumą elektroninėmis duomenų apdorojimo ir saugojimo priemonėmis, asmenišku paslaugų gavėjo prašymu ir paprastai už atlygį, kaip antai prieigos prie interneto, ryšių tinklo ir prieglobos paslaugas (šiuo klausimu žr. 2011 m. lapkričio 24 d. Sprendimo *Scarlet Extended*, C-70/10, EU:C:2011:771, 40 punktą; 2012 m. vasario 16 d. Sprendimo *SABAM*, C-360/10, EU:C:2012:85, 34 punktą; 2016 m. rugsėjo 15 d. Sprendimo *Mc Fadden*, C-484/14, EU:C:2016:689, 55 punktą; taip pat 2018 m. rugpjūčio 7 d. Sprendimo *SNB-REACT*, C-521/17, EU:C:2018:639, 42 punktą ir jame nurodytą jurisprudenciją).

199 Vis dėlto pagal Direktyvos 2000/31 1 straipsnio 5 dalį ši direktyva netaikoma sprendžiant klausimus, susijusius su informacinės visuomenės paslaugomis, kurias reglamentuoja direktyvos 95/46 ir 97/66. Šiuo klausimu iš Direktyvos 2000/31 14 ir 15 konstatuojamųjų dalių matyti, kad pranešimų konfidencialumo apsaugą ir fizinių asmenų apsaugą tvarkant asmens duomenis, susijusius su informacinės visuomenės paslaugomis, reglamentuoja tik Direktyva 95/46 ir Direktyva 97/66, o pastarosios 5 straipsnyje, siekiant apsaugoti pranešimų konfidencialumą, uždrausta bet kokia pranešimų perėmimo ar stebėjimo forma.

200 Taigi klausimai, susiję su pranešimų konfidencialumo ir asmens duomenų apsauga, turi būti vertinami atsižvelgiant į Direktyvą 2002/58 ir Reglamentą 2016/679, kuriais buvo pakeista atitinkamai Direktyva 97/66 ir Direktyva 95/46, pažymint, kad apsauga, kurią siekiama užtikrinti

Direktyva 2000/31, bet kuriuo atveju negali pažeisti iš Direktyvos 2002/58 ir Reglamento 2016/679 kylančių reikalavimų (šiuo klausimu žr. 2008 m. sausio 29 d. Sprendimo *Promusicae*, C-275/06, EU:C:2008:54, 57 punktą).

201 Taigi, kaip generalinis advokatas iš esmės pažymėjo savo išvados sujungtose bylose *La Quadrature du Net ir kt.* (C-511/18 ir C-512/18, EU:C:2020:6) 141 punkte, šio sprendimo 195 punkte nurodytais nacionalinės teisės aktais prieigos prie visuomenei skirtų ryšių paslaugų internetu ir prieglobos paslaugų teikėjams nustatyta pareiga saugoti asmens duomenis, susijusius su šiomis paslaugomis, turi būti vertinama atsižvelgiant į Direktyvą 2002/58 arba Reglamentą 2016/679.

202 Taigi, atsižvelgiant į tai, ar paslaugų, kurioms taikomi šie nacionalinės teisės aktai, teikimui taikoma Direktyva 2002/58, tokias paslaugas reglamentuoja arba pastaroji direktyva, visų pirma jos 15 straipsnio 1 dalis, siejama su Chartijos 7, 8 ir 11 straipsniais ir 52 straipsnio 1 dalimi, arba Reglamentas 2016/679, visų pirma jo 23 straipsnio 1 dalis, siejama su tomis pačiomis Chartijos nuostatomis.

203 Nagrinėjamu atveju negalima atmesti galimybės, kad, kaip savo rašytinėse pastabose pažymėjo Europos Komisija, kai kurios paslaugos, kurioms taikomi šio sprendimo 195 punkte nurodyti nacionalinės teisės aktai, yra elektroninių ryšių paslaugos, kaip jos suprantamos pagal Direktyvą 2002/58, o tai turi patikrinti prašymą priimti prejudicinį sprendimą pateikęs teismas.

204 Šiuo klausimu reikia pažymėti, kad Direktyva 2002/58 taikoma elektroninių ryšių paslaugoms, atitinkančioms Direktyvos 2002/21 2 straipsnio c punkte, į kurį daroma nuoroda Direktyvos 2002/58 2 straipsnyje ir kuriame elektroninių ryšių paslauga apibrėžiama kaip „paslauga, paprastai teikiama už atlygį, visa ar didžiąja dalimi susideda[nti] iš signalų perdavimo elektroninių ryšių tinklais, įskaitant telekomunikacijų paslaugas ir perdavimo paslaugas tinklais, naudojamais transli[uoti]“, nustatytas sąlygas. Informacinės visuomenės paslaugos, nurodytos šio sprendimo 197 ir 198 punktuose, kurioms taikoma Direktyva 2000/31, yra elektroninių ryšių paslaugos, nes jas visiškai arba daugiausia sudaro signalų perdavimas elektroninių ryšių tinklais (šiuo klausimu žr. 2019 m. birželio 5 d. Sprendimo *Skype Communications*, C-142/18, EU:C:2019:460, 47 ir 48 punktus).

205 Taigi prieigos prie interneto paslaugos, kurioms, atrodo, taikomi šio sprendimo 195 punkte nurodyti nacionalinės teisės aktai, yra, kaip patvirtinta Direktyvos 2002/21 10 konstatuojamojoje dalyje, elektroninių ryšių paslaugos, kaip jos suprantamos pagal šią direktyvą (šiuo klausimu žr. 2019 m. birželio 5 d. Sprendimo *Skype Communications*, C-142/18, EU:C:2019:460, 37 punktą). Tas pats pasakytina ir apie internetu teikiamas pašto paslaugas, kurios, atrodo, patenka ir į šių nacionalinės teisės aktų taikymo sritį, nes techniniu požiūriu jos visiškai ar iš esmės apima signalų perdavimą elektroninių ryšių tinklais (šiuo klausimu žr. 2019 m. birželio 13 d. Sprendimo *Google*, C-193/18, EU:C:2019:498, 35 ir 38 punktus).

206 Kiek tai susiję su reikalavimais, kylančiais iš Direktyvos 2002/58 15 straipsnio 1 dalies, siejamos su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, reikia nurodyti visas išvadas ir vertinimus, pateiktus atsakant į pirmuosius klausimus bylose C-511/18 ir C-512/18, taip pat į pirmąjį ir antrąjį klausimus byloje C-520/18.

207 Dėl iš Reglamento 2016/679 kylančių reikalavimų primintina, kad, kaip matyti iš 10 konstatuojamosios dalies, juo, be kita ko, siekiama užtikrinti vienodo ir aukšto lygio fizinių asmenų apsaugą visoje Sąjungoje ir šiuo tikslu užtikrinti nuoseklų ir vienodą taisyklių, reglamentuojančių šių asmenų pagrindinių teisių ir laisvių apsaugą tvarkant asmens duomenis, taikymą (šiuo klausimu žr. 2020 m. liepos 16 d. Sprendimo *Facebook Ireland ir Schrems*, C-311/18, EU:C:2020:559, 101 punktą).

208 Šiuo tikslu bet koks asmens duomenų tvarkymas, išskyrus Reglamento 2016/679 23 straipsnyje numatytas išimtis, turi būti atliekamas laikantis asmens duomenų tvarkymą reglamentuojančių principų, įtvirtintų šio reglamento II skyriuje, ir paisant jo III skyriuje numatytų duomenų subjektų

teisių. Konkrečiai kalbant, bet koks asmens duomenų tvarkymas turi, pirma, atitikti minėto reglamento 5 straipsnyje nurodytus principus ir, antra, tenkinti jo 6 straipsnyje numatytas teisėtumo sąlygas (kiek susiję su Direktyva 95/46, pagal analogiją žr. 2013 m. gegužės 30 d. Sprendimo *Worten*, C-342/12, EU:C:2013:355, 33 punktą ir jame nurodytą jurisprudenciją).

209 Konkrečiai dėl Reglamento 2016/679 23 straipsnio 1 dalies reikia pažymėti, kad pagal ją, kaip numatyta Direktyvos 2002/58 15 straipsnio 1 dalyje, valstybėms narėms, atsižvelgiant į joje numatytus tikslus, leidžiama, priimant teisėkūros priemones, apriboti direktyvoje numatytų pareigų ir teisių apimtį, „kai tokiu apribojimu paisoma pagrindinių teisių ir laisvių esmės ir jis demokratinėje visuomenėje yra būtina ir proporcinga priemonė siekiant užtikrinti“ numatytą tikslą. Bet kokia šiuo pagrindu priimta teisėkūros priemonė visų pirma turi atitikti konkrečius šio reglamento 23 straipsnio 2 dalyje nustatytus reikalavimus.

210 Taigi Reglamento 2016/679 23 straipsnio 1 ir 2 dalių negalima aiškinti kaip galinčių suteikti valstybėms narėms įgaliojimus pažeisti teisę į privataus gyvenimo gerbimą, nesilaikant Chartijos 7 straipsnio, kaip ir kitų Chartijoje numatytų garantijų (kiek tai susiję su Direktyva 95/46, pagal analogiją žr. 2003 m. gegužės 20 d. Sprendimo *Österreichischer Rundfunk ir kt.*, C-465/00, C-138/01 ir C-139/01, EU:C:2003:294, 91 punktą). Konkrečiai kalbant, kaip ir Direktyvos 2002/58 15 straipsnio 1 dalies atveju, pagal Reglamento 2016/679 23 straipsnio 1 dalį valstybėms narėms suteiktais įgaliojimais galima naudotis tik laikantis proporcingumo reikalavimo, pagal kurį nuo asmens duomenų apsaugos nukrypti leidžiančios nuostatos ir jų apribojimai neturi viršyti to, kas griežtai būtina (kiek tai susiję su Direktyva 95/46, pagal analogiją žr. 2013 m. lapkričio 7 d. Sprendimo *IPI*, C-473/12, EU:C:2013:715, 39 punktą ir jame nurodytą jurisprudenciją)

211 Vadinasi, išvados ir vertinimai, pateikti atsakant į pirmuosius klausimus bylose C-511/18 ir C-512/18, taip pat į pirmąjį ir antrąjį klausimus byloje C-520/18, *mutatis mutandis* taikomi Reglamento 2016/679 23 straipsniui.

212 Atsižvelgiant į tai, kas išdėstyta, į antrąjį klausimą byloje C-512/18 reikia atsakyti, kad Direktyva 2000/31 turi būti aiškinama taip, kad ji netaikoma pranešimų konfidencialumo apsaugai ir fizinių asmenų apsaugai tvarkant asmens duomenis, kiek tai susiję su informacinės visuomenės paslaugomis, nes tokia apsauga, atsižvelgiant į atvejį, reglamentuojama Direktyva 2002/58 arba Reglamentu 2016/679. Reglamento 2016/679 23 straipsnio 1 dalis, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad ja draudžiami nacionalinės teisės aktai, kuriais prieigos prie visuomenei skirtų ryšių paslaugų internetu teikėjai ir prieglobos paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai saugoti, be kita ko, su šiomis paslaugomis susijusius asmens duomenis.

Dėl trečiojo klausimo byloje C-520/18

213 Trečiuoju klausimu byloje C-520/18 prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės siekia išsiaiškinti, ar nacionalinis teismas gali taikyti nacionalinės teisės nuostatą, pagal kurią jam suteikta teisė apriboti laiko atžvilgiu jo paties pagal šią teisę neteisėtais pripažintų nacionalinės teisės aktų, kuriais elektroninių ryšių paslaugų teikėjai įpareigojami, atsižvelgiant, be kita ko, į nacionalinio saugumo užtikrinimo ir kovos su nusikalstamumu tikslus, bendrai ir nediferencijuotai saugoti srauto ir vietos nustatymo duomenis, poveikį, kai tokį neteisėtumą lemia teisės aktų neatitiktis Direktyvos 2002/58 15 straipsnio 1 daliai, siejamai su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi.

214 Pagal Sąjungos teisės viršenybės principą Sąjungos teisė laikoma viršesne už valstybių narių teisę. Taigi pagal šį principą reikalaujama, kad visos valstybių narių institucijos užtikrintų visišką įvairių Sąjungos teisės normų veiksmingumą, o valstybių narių teisė negali pakenkti šių įvairių normų veiksmingumui tų valstybių teritorijoje (1964 m. liepos 15 d. Sprendimas *Costa*, 6/64, EU:C:1964:66, p. 1159 ir 1160;

taip pat 2019 m. lapkričio 19 d. Sprendimo *A. K. ir kt. (Aukščiausiojo Teismo drausmės bylų kolegijos nepriklausomumas)*, C-585/18, C-624/18 ir C-625/18, EU:C:2019:982, 157 ir 158 punktai ir juose nurodyta jurisprudencija).

215 Pagal viršenybės principą nacionalinis teismas, įpareigotas taikyti Sąjungos teisės nuostatas pagal jam suteiktą jurisdikciją, tuo atveju, jei neturi įgaliojimų aiškinti nacionalinės teisės aktų atsižvelgdamas į Sąjungos teisės reikalavimus, turi pareigą užtikrinti visišką šių nuostatų veiksmingumą, prireikus savo iniciatyva netaikydamas jokios, net ir vėliau priimtos, joms prieštaraujančios nacionalinės teisės nuostatos, ir neprivalo prašyti, kad ši nacionalinė nuostata būtų panaikinta teisėkūros arba kitokiomis konstitucinėmis priemonėmis, arba laukti, kol tai bus padaryta (2010 m. birželio 22 d. Sprendimo *Melki ir Abdeli*, C-188/10 ir C-189/10, EU:C:2010:363, 43 punktas ir jame nurodyta jurisprudencija; 2019 m. birželio 24 d. Sprendimo *Popławski*, C-573/17, EU:C:2019:530, 58 punktas ir 2019 m. lapkričio 19 d. Sprendimo *A. K. ir kt. (Aukščiausiojo Teismo drausmės bylų kolegijos nepriklausomumas)*, C-585/18, C-624/18 ir C-625/18, EU:C:2019:982 160 punktas).

216 Tik Teisingumo Teismas išimties tvarka ir dėl imperatyvių teisinio saugumo pagrindų gali laikinai sustabdyti Sąjungos teisės normos naikinamąjį poveikį jai prieštaraujančios nacionalinės teisės normos atžvilgiu. Tokio Teisingumo Teismo pateikto šios teisės išaiškinimo veikimo laiko atžvilgiu ribojimas gali būti nustatytas tik pačiame sprendime, kuriame pateikiamas prašytas išaiškinimas (šiuo klausimu žr. 2012 m. spalio 23 d. Sprendimo *Nelson ir kt.* C-581/10 ir C-629/10, EU:C:2012:657, 89 ir 91 punktus; 2020 m. balandžio 23 d. Sprendimo *Herst*, C-401/18, EU:C:2020:295, 56 ir 57 punktus; taip pat 2020 m. birželio 25 d. Sprendimo *A ir kt. (Jėgainės Alteryje ir Nevelėje)*, C-24/19, EU:C:2020:503, 84 punktą ir jame nurodytą jurisprudenciją).

217 Jeigu nacionaliniai teismai turėtų įgaliojimus nors laikinai suteikti Sąjungos teisei prieštaraujančioms nacionalinėms nuostatoms viršenybę prieš Sąjungos teisę, būtų pakenkta Sąjungos teisės viršenybei ir vienodam jos taikymui (šiuo klausimu žr. 2019 m. liepos 29 d. Sprendimo *Inter-Environnement Wallonie ir Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, 177 punktą ir jame nurodytą jurisprudenciją).

218 Vis dėlto byloje, kurioje buvo nagrinėjamas priemonių, priimtų pažeidžiant Sąjungos teisėje įtvirtintą pareigą atlikti išankstinį projekto poveikio aplinkai ir saugomai teritorijai vertinimą, teisėtumas, Teisingumo Teismas nusprendė, kad nacionalinis teismas išimties tvarka gali, jei tai leidžiama pagal vidaus teisę, palikti galioti tokių priemonių padarinius, kai šis tolesnis taikymas pateisinamas privalomais pagrindais, susijusiais su būtinybe išvengti realios ir didelės grėsmės, kad atitinkamoje valstybėje narėje bus nutrauktas elektros energijos tiekimas, ir ši grėsmė negali būti pašalinta kitomis priemonėmis ar alternatyvomis, visų pirma vidaus rinkoje; palikti galioti minėtus padarinius galima tik tol, kol to neišvengiamai reikia tokiam neteisėtumui pašalinti (šiuo klausimu žr. 2019 m. liepos 29 d. Sprendimo *Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, 175, 176, 179 ir 181 punktus).

219 Priešingai nei tuo atveju, kai neįvykdyta procedūrinė pareiga, kaip antai išankstinis projekto poveikio konkrečioje aplinkos apsaugos srityje vertinimas, Direktyvos 2002/58 15 straipsnio 1 dalies, siejamos su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, pažeidimo negalima ištaisyti taikant procedūrą, panašią į nurodytąją ankstesniame punkte. Iš tiesų palikimas galioti nacionalinės teisės aktų, kaip nagrinėjami pagrindinėje byloje, poveikio reikštų, kad pagal šiuos teisės aktus elektroninių ryšių paslaugų teikėjams ir toliau nustatomi įpareigojimai, kurie prieštarauja Sąjungos teisei ir kuriais labai suvaržomos asmenų, kurių duomenys saugomi, pagrindinės teisės.

220 Vadinasi, prašymą priimti prejudicinį sprendimą pateikęs teismas negali taikyti savo nacionalinės teisės nuostatos, pagal kurią jis, remdamasis nacionaline teise, gali apriboti neteisėtais pripažintų pagrindinėje byloje nagrinėjamų nacionalinių teisės aktų poveikį laiko atžvilgiu.

221 Teisingumo Teismui pateiktose pastabose VZ, WY ir XX teigia, kad trečiuoju klausimu netiesiogiai, bet neišvengiamai keliama problema: ar pagal Sąjungos teisę draudžiama vykstant baudžiamajam procesui naudoti informaciją ir įrodymus, gautus bendrai ir nediferencijuojant saugant srauto ir vietos nustatymo duomenis, kai toks saugojimas yra nesuderinamus su Sąjungos teise.

222 Šiuo klausimu ir siekiant pateikti naudingą atsakymą prašymą priimti prejudicinį sprendimą pateikusiam teismui, reikia priminti, kad pagal šiuo metu galiojančią Sąjungos teisę iš principo tik nacionalinėje teisėje turi būti nustatytos taisyklės dėl informacijos ir įrodymų, gautų prieštaraujant Sąjungos teisei saugant duomenis, priimtinumo ir vertinimo baudžiamajame procese, pradėtame dėl sunkiomis nusikalstamomis veikomis įtariamų asmenų.

223 Iš Teisingumo Teismo suformuotos jurisprudencijos matyti, kad, jei nėra konkrečią sritį reglamentuojančių Sąjungos nuostatų, pagal procesinės autonomijos principą kiekvienos valstybės narės vidaus teisės sistemoje turi būti reglamentuotos ieškinių ir skundų, skirtų teisės subjektų iš Sąjungos teisės kildinamoms teisėms užtikrinti, procesinės taisyklės su sąlyga, kad jos nėra mažiau palankios nei taisyklės, reglamentuojančios panašias situacijas, kurioms taikoma vidaus teisė (lygiavertiškumo principas), ir kad dėl jų netampa praktiškai neįmanoma ar pernelyg sudėtinga pasinaudoti Sąjungos teisės suteiktomis teisėmis (veiksmingumo principas) (šiuo klausimu žr. 2015 m. spalio 6 d. Sprendimo *Târşia*, C-69/14, EU:C:2015:662, 26 ir 27 punktus; 2018 m. spalio 24 d. Sprendimo *XC ir kt.*, C-234/17, EU:C:2018:853, 21 ir 22 punktą bei juose nurodytą jurisprudenciją ir 2019 m. gruodžio 19 d. Sprendimo *Deutsche Umwelthilfe*, C-752/18, EU:C:2019:1114, 33 punktą).

224 Kiek tai susiję su lygiavertiškumo principu, nacionalinis teismas, nagrinėjantis baudžiamąją bylą, kurioje remiamasi informacija ir įrodymais, gautais pažeidžiant iš Direktyvos 2002/58 kylančius reikalavimus, turi patikrinti, ar šį procesą reglamentuojančioje nacionalinėje teisėje numatytos mažiau palankios taisyklės dėl tokios informacijos ir įrodymų priimtinumo ir naudojimo nei tos, kurios reglamentuoja pažeidžiant vidaus teisę gautą informaciją ir įrodymus.

225 Dėl veiksmingumo principo reikia pažymėti, kad nacionalinių taisyklių dėl informacijos ir įrodymų priimtinumo ir naudojimo tikslas, atsižvelgiant į pasirinktą nacionalinę teisę, yra neleisti, kad neteisėtai gauta informacija ir įrodymai nepagrįstai pakenktų asmeniui, įtariamam padarius nusikalstamas veikas. Vis dėlto pagal nacionalinę teisę šį tikslą galima pasiekti ne tik uždraudžiant naudoti tokią informaciją ir įrodymus, bet ir nacionalinėmis taisyklėmis ir praktika, reglamentuojančiomis informacijos ir įrodymų vertinimą ir svarbą, ar net atsižvelgiant į jų neteisėtumą paskiriant bausmę.

226 Iš Teisingumo Teismo jurisprudencijos matyti, kad būtinybė neįtraukti informacijos ir įrodymų, gautų pažeidžiant Sąjungos teisės reikalavimus, turi būti vertinama atsižvelgiant, be kita ko, į riziką, kurią tokios informacijos ir įrodymų priimtinumas gali sukelti rungimosi principo laikymuisi, taigi ir teisei į teisingą bylos nagrinėjimą (šiuo klausimu žr. 2003 m. balandžio 10 d. Sprendimo *Steffensen*, C-276/01, EU:C:2003:228, 76 ir 77 punktus). Teismas, kuris mano, kad šalis negali veiksmingai pateikti pastabų dėl įrodinėjimo priemonės, kuri priklauso teisėjams nežinomai sričiai ir gali daryti lemiamą įtaką faktinių aplinkybių vertinimui, turi konstatuoti teisės į teisingą bylos nagrinėjimą pažeidimą ir atmesti šį įrodymą, kad būtų išvengta tokio pažeidimo (šiuo klausimu žr. 2003 m. balandžio 10 d. Sprendimo *Steffensen*, C-276/01, EU:C:2003:228, 78 ir 79 punktus)

227 Vadinasi, pagal veiksmingumo principą nacionalinis baudžiamųjų bylų teismas, vykstant baudžiamajam procesui, pradėtam dėl nusikalstamomis veikomis įtariamų asmenų, privalo neatsižvelgti į informaciją ir įrodymus, gautus atliekant su Sąjungos teise nesuderinamą bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, jeigu šie asmenys negali veiksmingai pateikti pastabų dėl šios informacijos ir įrodymų, kurie priklauso teisėjams nežinomai sričiai ir gali daryti lemiamą įtaką faktinių aplinkybių vertinimui.

228 Atsižvelgiant į tai, kas išdėstyta, į trečiąjį klausimą byloje C-520/18 reikia atsakyti taip, kad nacionalinis teismas negali taikyti nacionalinės teisės nuostatos, pagal kurią jam suteikta teisė apriboti laiko atžvilgiu jo paties pagal šią teisę neteisėtais pripažintų nacionalinės teisės aktų, kuriais elektroninių ryšių paslaugų teikėjai įpareigojami, atsižvelgiant, be kita ko, į nacionalinio saugumo užtikrinimo ir kovos su nusikalstamumu tikslus, taikyti bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, nesuderinamą su Direktyvos 2002/58 15 straipsnio 1 dalimi, siejama su Chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, poveikį. Pagal šio 15 straipsnio 1 dalį, aiškinamą atsižvelgiant į veiksmingumo principą, nacionalinis baudžiamųjų bylų teismas, vykstant baudžiamajam procesui, pradėtam dėl nusikalstamomis veikomis įtariamų asmenų, privalo neatsižvelgti į informaciją ir įrodymus, gautus atliekant su Sąjungos teise nesuderinamą bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, jeigu šie asmenys negali veiksmingai pateikti pastabų dėl šios informacijos ir įrodymų, kurie priklauso teisėjams nežinomai sričiai ir gali daryti lemiamą įtaką faktinių aplinkybių vertinimui.

Dėl bylinėjimosi išlaidų

229 Kadangi šis procesas pagrindinių bylų šalims yra vienas iš etapų prašymą priimti prejudicinį sprendimą pateikusių teismų nagrinėjamose bylose, bylinėjimosi išlaidų klausimą turi spręsti šie teismai. Išlaidos, susijusios su pastabų pateikimu Teisingumo Teismui, išskyrus tas, kurias patyrė minėtos šalys, nėra atlygintinos.

Remdamasis šiais motyvais, Teisingumo Teismas (didžioji kolegija) nusprendžia:

1. **2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvos 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), iš dalies pakeistos 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos direktyva 2009/136/EB, 15 straipsnio 1 dalis, siejama su Europos Sąjungos pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją draudžiamos teisėkūros priemonės, kuriomis, siekiant šio 15 straipsnio 1 dalyje numatytų tikslų, prevenciškai numatomas bendras ir nediferencijuotas srauto ir vietos nustatymo duomenų saugojimas. Vis dėlto pagal Direktyvos 2002/58, iš dalies pakeistos Direktyva 2009/136, 15 straipsnio 1 dalį, siejamą su Pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, nedraudžiamos tokios teisėkūros priemonės:**

   – **kuriomis, siekiant užtikrinti nacionalinį saugumą, leidžiama įpareigoti elektroninių ryšių paslaugų teikėjus bendrai ir nediferencijuojant saugoti srauto ir vietos nustatymo duomenis tais atvejais, kai atitinkama valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra, esama arba numatoma, o sprendimui, kuriame nustatytas toks įpareigojimas, gali būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja viena iš tokių situacijų, taip pat, ar laikomasi sąlygų ir garantijų, kurios turi būti numatytos; toks įpareigojimas gali būti nustatytas tik laikotarpiui, neviršijančiam to, kas griežtai būtina, bet jeigu grėsmė išlieka, galimam pratęsti,**

   – **kuriomis, siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiomis nusikalstamomis veikomis ir užkirsti kelią didelei grėsmei visuomenės saugumui, numatomas tikslinis srauto ir vietos nustatymo duomenų saugojimas, kuris, remiantis objektyviais ir nediskriminaciniais veiksniais, atsižvelgiant į duomenų subjektų kategorijas arba geografinius kriterijus, būtų apribotas laikotarpio, neviršijančio to, kas griežtai būtina, tačiau kurį galima pratęsti,**

– **kuriomis, siekiant užtikrinti nacionalinį saugumą, kovoti su sunkiomis nusikalstamomis veikomis ir užkirsti kelią didelei grėsmei visuomenės saugumui, numatomas bendras ir nediferencijuotas ryšio šaltinio IP adresų saugojimas laikotarpiu, neviršijančiu to, kas griežtai būtina,**

– **kuriomis, siekiant užtikrinti nacionalinį saugumą, kovoti su nusikalstamumu ir užtikrinti visuomenės saugumą, numatomas bendras ir nediferencijuotas duomenų, susijusių su elektroninių ryšių priemonių naudotojų civiline tapatybe, saugojimas ir**

– **kuriomis, siekiant kovoti su sunkiomis nusikalstamomis veikomis ir *a fortiori* užtikrinti nacionalinį saugumą, leidžiama kompetentingos institucijos, kuriai taikoma veiksminga teisminė kontrolė, sprendimu įpareigoti elektroninių ryšių paslaugų teikėjus apibrėžtu laikotarpiu užtikrinti operatyvų srauto ir vietos nustatymo duomenų, kuriuos turi šie paslaugų teikėjai, saugojimą,**

kai tokios priemonės aiškiomis ir tiksliomis taisyklėmis užtikrina, kad saugant nagrinėjamus duomenis būtų laikomasi su tokiu saugojimu susijusių materialinių ir procesinių sąlygų ir atitinkami asmenys turėtų veiksmingas garantijas nuo piktnaudžiavimo rizikos.

2. **Direktyvos 2002/58, iš dalies pakeistos Direktyva 2009/136, 15 straipsnio 1 dalis, siejama su Pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad pagal ją nedraudžiamos nacionalinės teisės nuostatos, kuriomis elektroninių ryšių paslaugų teikėjai įpareigojami, pirma, vykdyti srauto ir vietos nustatymo duomenų automatizuotą analizę bei jų rinkimą realiuoju laiku ir, antra, realiuoju laiku rinkti techninius duomenis, susijusius su galinių įrenginių vieta, jeigu:**

– **automatizuota analizė atliekama tik tais atvejais, kai valstybė narė susiduria su didele grėsme nacionaliniam saugumui, kuri yra tikra ir esama arba numatoma, o tokios analizės atlikimui turi būti taikoma veiksminga teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant patikrinti, ar egzistuoja minėtą priemonę pateisinanti situacija ir ar laikomasi sąlygų ir garantijų, kurios turi būti numatytos, ir jeigu**

– **srauto ir vietos nustatymo duomenų rinkimas realiuoju laiku taikomas tik tiems asmenims, dėl kurių yra pagrįsta priežastis įtarti, kad jie vienaip ar kitaip susiję su terorizmo veikla, ir jeigu tokiam duomenų rinkimui taikoma išankstinė teismo arba nepriklausomos administracinės institucijos, kurios sprendimas turi privalomąją galią, kontrolė, siekiant įsitikinti, kad toks duomenų rinkimas realiuoju laiku leidžiamas tik tiek, kiek tai griežtai būtina. Tinkamai pagrįstos skubos atveju kontrolė turi būti vykdoma per trumpą laiką.**

3. **2000 m. birželio 8 d. Europos Parlamento ir Tarybos direktyva 2000/31/EB dėl kai kurių informacinės visuomenės paslaugų, ypač elektroninės komercijos, teisinių aspektų vidaus rinkoje (Elektroninės komercijos direktyva) turi būti aiškinama taip, kad ji netaikoma pranešimų konfidencialumo apsaugai ir fizinių asmenų apsaugai tvarkant asmens duomenis, kiek tai susiję su informacinės visuomenės paslaugomis, nes tokia apsauga, atsižvelgiant į atvejį, reglamentuojama Direktyva 2002/58, iš dalies pakeista Direktyva 2009/136, arba 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46. Reglamento 2016/679 23 straipsnio 1 dalis, siejama su Pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, turi būti aiškinama taip, kad ja draudžiami nacionalinės teisės aktai, kuriais prieigos prie visuomenei skirtų ryšių paslaugų internetu teikėjai ir prieglobos paslaugų teikėjai įpareigojami bendrai ir nediferencijuotai saugoti, be kita ko, su šiomis paslaugomis susijusius asmens duomenis.**

4. Nacionalinis teismas negali taikyti nacionalinės teisės nuostatos, pagal kurią jam suteikta teisė apriboti laiko atžvilgiu jo paties pagal šią teisę neteisėtais pripažintų nacionalinės teisės aktų, kuriais elektroninių ryšių paslaugų teikėjai įpareigojami, atsižvelgiant, be kita ko, į nacionalinio saugumo užtikrinimo ir kovos su nusikalstamumu tikslus, taikyti bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, nesuderinamą su Direktyvos 2002/58, iš dalies pakeistos Direktyva 2009/136, 15 straipsnio 1 dalimi, siejama su Pagrindinių teisių chartijos 7, 8, 11 straipsniais ir 52 straipsnio 1 dalimi, poveikį. Pagal šio 15 straipsnio 1 dalį, aiškinamą atsižvelgiant į veiksmingumo principą, nacionalinis baudžiamųjų bylų teismas, vykstant baudžiamajam procesui, pradėtam dėl nusikalstamomis veikomis įtariamų asmenų, privalo neatsižvelgti į informaciją ir įrodymus, gautus atliekant su Sąjungos teise nesuderinamą bendrą ir nediferencijuotą srauto ir vietos nustatymo duomenų saugojimą, jeigu šie asmenys negali veiksmingai pateikti pastabų dėl šios informacijos ir įrodymų, kurie priklauso teisėjams nežinomai sričiai ir gali daryti lemiamą įtaką faktinių aplinkybių vertinimui.

Parašai.